جامعة يحيى فارس بالمدية

كلية الحقوق والعلوم السياسية

مكافحة الجريمة المعلوماتية

(دراسة مقارنة بين التشريع الجزائري والتشريع الفلسطيني)

مذكرة لنيل شهادة ماستر في الحقوق
تخصص: القانون الجنائي والعلوم الجنائية

من إعداد الطالب:

- خالد عطية عارف فرّاج

تحت إشراف الأستاذ:

- د. إحسان طبال

أعضاء لجنة المناقشة:

د/ مزعد إبراهيم	**رئيساً**
د/ إحسان طبال	**مشرفاً ومقرراً**
د/ عمري عبد القادر	**مناقشاً**

السنة الجامعية 2018/2017

شكـر وعرفــان

الحمدلله الذي أنار لنا درب العلم والمعرفة ووفقني على أداء هذا العمل،

فالشكر لله دائماً وأبدا...

وأتقدم بالشكر الجزيل والإمتنان للدكتور **المشرف إحسان طبال** على جهده المبذول وتوجيهاته القيّمة طوال فترة إنجاز المذكرة...

والشكر الموصول لأعضاء لجنة المناقشة...

د/ مزعد إبراهيم رئيساً ، د/ عمري عبد القادر مناقشاً

وأشكر كل من ساعدني في إتمام هذه المذكرة من قريب أو من بعيد...

ولا يفوتني أن أشكر معلّمي في فلسطين وأساتذتي في جامعة المدية وجامعة الأغواط...

الإهـــداء

" وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ " صدق الله العظيم

إلى رَجُلٍ رحلت معه أسمى معاني الحياة، إلى من علمني كيف أصارع فهم الحياة وأصعد سلم النجاح خطوة بخطوة، إلى من إرتسم على جبينه تجعدات التعب لأصل إلى هذا اليوم... والدي العزيز. لك الرحمة.

إلى من أُطفِئَت عيونها لتنير لي ظلمات المستقبل، وأهدتني عمراً من الحنان والسهر والدعاء، وكانت لي الشمعة التي أنارت بدعائها غربتي لأصل إلى هذا اليوم.. أمي الغالية

إلى ستة أقمار كانوا لي السّد الذي أحتمي به، ووقفوا بجانبي طيلة فترة غربتي لأصل إلى هذا اليوم... أُخواني الأعزاء

إلى رفاق جمعتني بهم الغربة فكانوا إخوةً، وإلى أصدقاء غبت عنهم سنوات فلم ينسوني بدعائهم لأصل إلى هذا اليوم... أصدقاء الغربة... أصدقاء الطفولة

هل سأراك سالماً منعماً، وغانماً مكّرماً، غربتي لأجلك، وتعبي لأجلك، وعمري فداك... بلدي فلسطين

إلى من احتوتني واحتضنتني، عرفت بها أصالتها وعراقتها وطيبة أهلها فكانت لي بلدي الثاني... الجزائر الحبيبة

فـــرّاج خالـــد

مقدمة

نظراً لما يشهده العالم من تطور على المستوى العلمي والتكنولوجي، فإن إدخال تكنولوجيا المعلومات في حياتنا اليومية قد يكون سيفاً ذو حدين، فمن جهة تعمل تكنولوجيا المعلومات على تسهيل المعاملات اليومية، وتوفير الجهد والوقت، ومن جهة أخرى فإن هذه الوسائل التكنولوجية لم تسلم من الظواهر الإجرامية فقد أصبحت مجالاً خصباً لارتكاب الجرائم فيها، كجرائم قرصنة المعلومات والمواقع الإلكترونية، وجرائم غسل الأموال التي تتم عن طريق التحويل الإلكتروني للأموال، وجرائم الابتزاز والتشهير والقذف على وسائل التواصل الاجتماعي، الأمر الذي أصبح يهدد كل من يستخدم هذه الوسائل، لذلك كان لزاماً على المشرع الجزائري والفلسطيني التدخل من أجل حماية هذا المجال وحماية مستخدميه، وذلك من خلال سن نصوص جنائية تجرّم بعض الأفعال التي يتم إتيانها من خلال وسائل التكنولوجيا على وجه الخصوص أو التي ترتكب على المعلوماتية بصفة عامة.

ونظراً لحداثة الجريمة المعلوماتية، فكانت الدول لم تشهد هذا النوع من الجرائم، مما جعل القوانين غير فعالة في مواجهة مرتكبيها في ظل فقدان الشرعية الجنائية، ومع انتشار هذا النوع من الجرائم قامت الدول بإحاطتها بقوانين خاصة في مكافحة الجريمة المعلوماتية، أو قيامها بإدراج نصوص ضمن قانون العقوبات لمعالجة هذه الجريمة ومكافحتها، وهو الأمر الحاصل في عديد من الدول لا سيما العربية منها لكي تتماشى تشريعاتها مع ما هو مستحدث من ظواهر إجرامية.

تكمن أهمية هذا الموضوع بالنظر إلى مدى ملائمة وكفاية النصوص القانونية في المكافحة والتصدي للجريمة المعلوماتية في ظل التطور السريع لوسائل تكنولوجيا المعلومات التي أصبحت تشكل جزءاً أساسياً من حياة الأفراد، فتلك الوسائل لم تسلم من الإجرام فأصبحت بيئة لارتكاب الجرائم فيها.

ويكتسي موضوع المذكرة أهمية بالغة أيضاً من حيث أنه يسلط الضوء على النصوص الموضوعية والقواعد الإجرائية التي تكفل الحماية ومعاقبة المجرمين الذين قاموا بأي انتهاكات ضد أنظمة المعلوماتية بشكل تقوم معه الجريمة المعلوماتية، فقد أصبح الفضاء السيبراني مجالاً لارتكاب الجرائم المعلوماتية، كجرائم قرصنة المعلومات، غسل الأموال، وغيرها من الجرائم المعلوماتية.

تختلف الطبيعة القانونية للجريمة المعلوماتية عن الطبيعة القانونية للجرائم التقليدية التي ترتكب على أرض الواقع وتكون ذات طابع مادي وملموس، فالجريمة المعلوماتية هي جريمة ترتكب

في الفضاء السيبراني فهي لا تخلّف آثاراً مادية على أرض الواقع، لذلك فهي ذات طبيعة خاصة، ونظراً لطبيعتها كان لا بدّ من استحداث نصوصاً خاصة تنظم أحكامها من الناحيتين التجريمية والإجرائية، فقد كان لكلا المشرعين الجزائري والفلسطيني نظرة خاصة في التعامل مع هذا النوع من الجرائم، فأردنا من خلال هذا البحث تسليط الضوء على الأحكام الخاصة بهذه الجريمة في كل من القانونين الجزائري والفلسطيني.

وتهدف الدراسة إلى الوقوف على الحماية الجنائية من الجريمة المعلوماتية في قانون العقوبات، و قد تختلف هذه الحماية من قانون إلى آخر فقانون العقوبات الجزائري يختلف عن قانون العقوبات المطبق في فلسطين من حيث أحكامه ونظرته التجريمية من أجل فرض حماية جنائية كفيلة للحد من ظاهرة الإجرام السيبراني، فما يعتبر جريمة في قانون العقوبات الجزائري قد لا يكون كذلك في قانون العقوبات المطبق في فلسطين.

فبعد ارتكاب الفعل المجرم تبدأ عملية القيام بالإجراءات القانونية المنصوص عليها في قانون الإجراءات الجزائية، بحيث يعتبر عوناً لقانون العقوبات في تحقيق الدفاع الاجتماعي ضد الجريمة، وهو يعتبر دستور الحريات لما يحتويه من ضمانات فردية للمشتبه فيهم أو المتهمين بارتكاب جرائم ما، ويضع الإجراءات التي تلازم وقوع الجريمة إلى حين إلقاء القبض على مرتكبها وتقديمه للعدالة.

وفي سياق متصل يأتي دور الجهات القائمة على تنفيذ الإجراءات عموماً، التي تلتزم بالنطاق الجغرافي الممنوح لها بموجب القانون والذي تمارس عليه صلاحياتها في مجال البحث والتحري عن الجرائم المعلوماتية، ويحدد هذا القانون الإجراءات الواجب اتخاذها في بعض الجرائم الخاصة كالجريمة المعلوماتية، وبعض القوانين تركتها للقواعد الكلاسيكية في التحقيق الجنائي كالقانون الفلسطيني.

كما أصبح لزاماً تبيان أوجه الحماية في القوانين النافذة في كلا الدولتين الجزائرية والفلسطينية، كلٌ حسب رؤيته التي يراها مناسبة في مكافحة ظاهرة الإجرام المعلوماتي.

ومن الأسباب التي دفعتني لإختيار الموضوع، الاهتمام الشخصي في مجال المعلوماتية كظاهرة إجرامية منتشرة على مستوى العالم والتي يمكن أن تمس أي شخص طالما يستخدم وسائل تكنولوجيا المعلومات، هذا بالإضافة إلى الحداثة التي تتمتع بها الجريمة المعلوماتية دفعتني إلى تناولها بالدراسة، ونظراً لحداثة القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية

الفلسطيني أدى بي إلى البحث في هذا المجال، بالإضافة إلى محاولة نقل النظرة الجزائرية في مجال مكافحة الإجرام المعلوماتي لفلسطين من خلال هذا البحث العلمي.

حيث أنه من بين الصعوبات التي واجهتني في إعداد هذا البحث، قلة المراجع والدراسات المتخصصة في المجال المعلوماتي، كذلك صعوبة التواصل مع جهات البحث والتحري في فلسطين من أجل الحصول على معلومات بشأن الدراسة فقد حالت المسافة عائقاً بيننا وبينهم.

اعتمد الباحث على المنهج المقارن بصفة أساسية بين القانون الجزائري والقانون الفلسطيني بالإضافة إلى المنهج الوصفي باستخدام أدوات التحليل وذلك لإعطاء صورة كاملة ومتكاملة عن النصوص القانونية التي تناولت الجريمة المعلوماتية ولتبيان معالمها وواقعها في كلا التشريعين الجزائري والفلسطيني على حد السواء.

ولذلك يطرح الموضوع إشكالية تتمثل في "**مدى فاعلية النصوص الجنائية الوطنية في التشريع الجزائري مقارنةً بالتشريع الفلسطيني في مواجهة الجريمة المعلوماتية والحد من خطورتها**"؟

وجواباً على الإشكالية المطروحة ارتأينا تقسيم الدراسة إلى فصلين تناولنا في **الفصل الأول الإطار الموضوعي للجريمة المعلوماتية**، وقسمناه إلى مبحثين، المبحث الأول جاء تحت عنوان المكافحة الموضوعية للجريمة المعلوماتية في ظل قانون العقوبات، بينما المبحث الثاني المكافحة الموضوعية للجريمة المعلوماتية في ظل القوانين الخاصة، وتناولنا في **الفصل الثاني الإطار الإجرائي للجريمة المعلوماتية**، وقسمناه إلى مبحثين كذلك، **الأول** جاء تحت عنوان المكافحة الإجرائية للجريمة المعلوماتية في ظل قانون الإجراءات الجزائية، بينما **المبحث الثاني** المكافحة الإجرائية في ظل القوانين الخاصة.

الفصل الأول

الإطار الموضوعي للجريمة المعلوماتية

تمهيد:

تختلف التشريعات الجنائية في التجريم من حيث اختلاف النصوص المتعلقة بتجريم الأفعال وكذلك العقوبات المقررة لكل جريمة من تشريع إلى اخر ، ونظرا لخصوصية الجريمة المعلوماتية وحداثتها وتطورها أدى إلى اختلاف التشريعات في معالجة هذه الجريمة ومواجهتها من خلال تجريم الافعال على اوسع نطاق كي تتمكن الدول من مكافحة وردع هذا النوع من الجرائم، ولعل السبب في ذلك يعود لما يتميز به مرتكبو الجريمة المعلوماتية من دراية في المجال الالكتروني وذكاء في ارتكابها كونها جريمة لا تتسم بالعنف وتتسم بالهدوء والحاق الضرر بالضحية بحسب النية الاجرامية للجاني.

وحداثة هذه الجريمة ومساسها بالأفراد أو الدولة أو الأشخاص المعنوية وإلحاق الضرر بها على جميع الاصعدة دفعنا إلى دراسة مكافحة هذه الجريمة من خلال الشرعية الجنائية في قانون العقوبات وكذا القوانين الخاصة لتحديد نطاق هذه المكافحة الموضوعية ومدى شموليتها لصور هذه الجريمة، وهذا ما سنتناوله في المبحث الأول المكافحة الموضوعية للجريمة المعلوماتية في قانون العقوبات، في المطلب الأول تطويع النصوص الجنائية التقليدية، وفي المطلب الثاني استحداث نصوص جنائية خاصة تعنى بالجريمة المعلوماتية، أما المبحث الثاني المكافحة الموضوعية للجريمة المعلوماتية في ظل القوانين الخاصة، المطلب الأول الحماية الجنائية في القوانين المكملة لقانون العقوبات، والمطلب الثاني الحماية الجنائية في النصوص المتعلقة بالملكية الفكرية والمعاملات الالكترونية.

المبحث الأول

المكافحة الموضوعية للجريمة المعلوماتية في قانون العقوبات

تتعلق المكافحة الموضوعية أساساً في النصوص الجنائية المتعلقة بالجريمة المعلوماتية في كلا التشريعين الجزائري والفلسطيني وكذا العقوبات التي يقررها كلا التشريعين لهذا النوع من الجرائم، وكيف تم التعامل مع الجريمة من منظور قانون العقوبات خاصة عندما لا ينص القانون صراحة على تجريم الفعل وارتكابه باستخدام التقنية المعلوماتية وهنا يتعلق الامر بتطويع النصوص الجنائية التقليدية أو الكلاسيكية في مدى اعتبار جرائم المعلوماتية من قبيل جرائم الأموال من عدمه هذا من جهة، ومن جهة اخرى وفي ظل قصور التشريع على اصباغ الحماية الجنائية على الافعال التي تعتبر من قبيل الجرائم المعلوماتية قام كلا المشرعين باستحداث نصوص تتعلق بالجريمة المعلوماتية بصورة مباشرة. وقسمنا هذا المبحث إلى مطلبين الأول تحت عنوان تطويع النصوص الجنائية التقليدية، أما المطلب الثاني جاء تحت عنوان ضرورة استحداث نصوص جنائية خاصة تعنى بالجريمة المعلوماتية.

المطلب الأول: تطويع النصوص الجنائية التقليدية

تعتبر الوسائط الإلكترونية ناقلاً هاماً للمعلومات وتخزينها ومعالجتها، وقابلية ربطها مع العديد من الشبكات المعلوماتية، الأمر الذي سهّل الوصول إليها من طرف المعني بها، مما فتح المجال لارتكاب الجرائم فيها، وبالنظر للقيمة الاقتصادية للمعلوماتية اصبح لابد من حمايتها جزائيا ليرتدع مرتكبو هذه الجرائم ومواجهتهم بالتجريم والعقاب، وهو ما نادى به الفقهاء والباحثين، ومن هنا يثور التساؤل حول امكانية تطبيق النصوص القانونية لإضفاء الحماية الجنائية على استعمال المعلوماتية من خلال جرائم الأموال؟

الفرع الأول: مدى انطباق وصف المال على المعلوماتية

عرفت المادة 682 فقرة 1 من القانون المدني الجزائري المال بأنه :" **كل شيء غير خارج عن التعامل بطبيعته أو بحكم القانون**"[1]، والشيء في نظر القانون هو " كل ما يصلح ان يكون

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المعدّل والمتمم، المادة 682.

محلا للذمة المالية"، فالشيء غير المال، والمال هو الحق الذي يرد على الشيء، او هو الحق ذو القيمة المالية، والشيء هو عبارة عن محل الحق المالي، وفي الجهة المقابلة نستعرض تعريف المشرع الفلسطيني للمال في المادة 64 من مشروع القانون المدني الفلسطيني والتي تنص على " **كل شيء لا يخرج عن التعامل بطبيعته أو بحكم القانون يصح أن يكون محلاً للحقوق المالية**"[1].

والشيء قد يكون ماديا أو معنويا ، بحيث أن الأول يمثل موضوع الحق العيني، أما الثاني يمثل موضوع الحق الذهني، كما أن الأموال تنقسم إلى اموال مادية واموال معنوية.

من الواضح ان التشريعات التي استخدمت مصطلح "المال" كانت اكثر توفيقا من غيرها التي استعملت مصطلح "الشيء" كون أن دلالة المال واضحة ودقيقة على عكس الشيء، ولتحديد وصف الشيء يذهب الاستاذين ميرل وفيتي merle et vête إلى القول بأن كلمة الشيء الواردة في المادة 379 من قانون العقوبات الفرنسي تدل على الأشياء المادية الملموسة[2].

بناء على ما سبق نرى بأن هناك اتجاه يضفي على الشيء مصطلح المال، فبمجرد ثبوت صفة المال على الشيء يمكن تطبيق الجرائم التقليدية عليه وذلك لشمولية لفظ المال، وبالرجوع إلى النظرة التقليدية لجرائم الأموال نرى بأن هذه الجرائم لا ترد إلا على الأشياء المادية الملموسة والسبب في ذلك يعود إلى كثرتها في ذلك الوقت، أما الأشياء المعنوية نظراً لقلتها تم تحييدها من طرف المشرعين وحصر جرائم الأموال في الأشياء المادية الملموسة فقط.

غير أنه بالنظر إلى التطور الحاصل للأشياء المعنوية والتي أصبحت أكبر عدداً مما كان في السابق، وأصبحت تفوق من حيث قيمتها الأشياء المادية في حد ذاتها، مما أدى إلى التراجع عن القول بأن الأموال تنحصر في الأشياء المادية والبحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي، حتى يتم اضفاء صفة المال على الأشياء المعنوية، ومن هذه الأشياء المعنوية مثلاً المعلومات ذات القيمة الاقتصادية العالية، وتبعاً إلى طبيعة هذه المعلومات نجد بأنها مالا ذو طابع معنوي، إلا أنه وفقا للاتجاه التقليدي لا يمكن اضفاء صفة المال عليها، مما يعني أنه لا يمكن أن تكون محلا لجرائم الأموال في حالة الرجوع إلى النصوص التقليدية القائمة، إلا إذا كانت هذه المعلومات مثبتة على دعامة مادية أو حامل Support ومنها: الأقراص الممغنطة C.D أو الشرائط

---

(1) دولة فلسطين، القانون المدني الفلسطيني رقم 4 لسنة 2012 المؤرخ في 2012/8/5، جريدة الوقائع الفلسطينية عدد ممتاز، المادة 64.

(2) خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، طبعة 2010، دار الهدى، الجزائر، 2010،ص 36،ص37.

Flash Disc أو بطاقة الذاكرة Memory card ، وعليه فإن الاعتداء يقع على الدعامة كونها شيئاً مادياً يمكن أن تطبق عليه النصوص التقليدية، حتى وإن كانت الغاية من الاعتداء ليست الدعامة بل المعلومات، إلا أن القانون الجنائي لا يعتد بهذه البواعث[1].

لهذا اختلف الفقه الجنائي في اعتبار المعلومات من قبيل المال استناداً إلى أن المعلومات ليست من قبيل الأشياء بحيث أن جرائم الأموال لا تحمي سوى المنقولات، وهذه الاخيرة لا تثبت لها هذه الصفة إلا اذا كانت من الأشياء، والفارق كبير بين الأشياء والأفكار أو المعلومات[2].

في حقيقة الأمر أن الجريمة المرتكبة كسرقة الدعامة مثلاً، ما كانَ ليتم ارتكاب هذه الجريمة لولا وجود المعلومات على الدعامة، وبالتالي فإن القول بأن الإعتداء على المعلومات يخرج من نطاق التجريم هو قول غير سليم، كون أن المجرم الذي يسرق دعامة تحتوي على معلومات سرية لمؤسسة حكومية يعاقب بعقوبة بسيطة أو يمنع من العقاب وذلك لنظرة المشرع للمال المسروق وهو الدعامة ولم ينظر للمعلومات، لذلك فإن هذا القول غير سليم، بل يجب على المشرع ان يعتد بالباعث في مثل هذه الحالات[3].

ويبقى الإشكال المطروح في الحالة التي يقع فيها الإعتداء على المعلومات التي تكون مستقلة عن دعامتها، على اعتبار أن الإعتداء وقع على شيء معنوي. كما سبق قوله بأنه كي يتم تطبيق النصوص المتعلقة بجرائم الأموال يجب أن يثبت للشيء وصف المال وإلا لا يمكن تطبيق تلك النصوص على الفعل، وقد انقسم الفقه بين مؤيد ومعارض لفكرة إضفاء صفة المال على المعلومات من عدمه وهو ما سنتعرض له على النحو الاتي:

أولاً: مؤيدو إضفاء وصف المال على المعلوماتية

يرى جانب من الفقه بأن المعلوماتية تتسم بوصف المال وذلك على اساس انها نتاج خاص بمن فكر بها وهي تعكس الراي الشخصي لصاحبها وبالتالي فهي احدى الحقوق اللصيقة بالشخصية وهو ما يعطيها خاصية الانتقال فهي قابلة للانتقال من شخص إلى اخر اي من مرسل

(1) خثير مسعود، مرجع سابق، ص37،ص38.
(2) حجازي عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، بدون رقم طبعة، دار النهضة العربية، مصر، 2009، ص422.
(3) خثير مسعود، مرجع سابق، ص38.

إلى مستقبل ومن هذا المنطلق فإنه يمكن للشخص الاستئثار بها والتصرف فيها او استغلالها[1] وهذا الجانب من الفقه يستبعد المعلومات التي لا تظهر في شكل قوالب مادية، وذلك كون أن الفكرة في ذهن صاحبها ليس لها نظام قانوني ما لم يتم الافصاح عنها على ارض الواقع بأي شكل من الاشكال القابلة للحماية من طرف القانون، كون ان المعلومات في ذهن صاحبها تأخذ حكم النية والقانون الجنائي لا يعتد بالنوايا والسرائر ما لم يتم البدء بالتنفيذ على ارض الواقع وبالتالي يتم استبعادها من نطاق التجريم.

وفي سياق متصل ذهب هذا الجانب من الفقه إلى القول بأن " المعلومات ما هي الا مجموعة القيم المستحدثة"، ولعل الفضل في ذلك يعود إلى الاستاذين فيفا وكاتالا gatala et vivant ، حيث يرى الاستاذ كاتالا: "**أن المعلومة المستقلة عن دعامتها المادية تكون لها قيمة قابلة للاستحواذ وذلك لأنها قيم وفقاً لسعر السوق متى كانت غير محظورة تجاريا، كما وانها منهج بصرف النظر عن دعامتها المادية عن عمل من قدمها**"[2]، وعلى هذا الاساس تنشأ علاقة محورها المعلومات إما بينها وبين صاحبها او بين صاحبها والغير، وباعتبار ان المعلومات هي نتاج ذهني لمن يعطيها شكل المعلومة ، ينشا عنها علاقة كالعلاقة التي تنشا بين المالك وبين ما يملك فيكون له نقلها وايداعها وحفظها وتأجيرها وبيعها كما تتولد عنها وتتغير وتنتهي حقوقا عليها ومن بين هذه المعلومات هو برامج الكمبيوتر[3].

فإذا كان الفقه التقليدي قد استبعد المعلومات من طائفة الأموال كونها غير مادية، فإن الفقه الحديث اعترف بوصف المال على المعلومات على اساس أن هذه المعلومات تمنح لمالكها حقوقا كعقد الايجار او البيع وما إلى ذلك من الحقوق، وذلك بالنظر لتلك العلاقة التي تنشا بين المعلومة ومالكها، بالإضافة إلى القيمة الاقتصادية لتلك المعلومات وهذا ما نادى به الاستاذ كاربونيه– carbonnier في دراسته المتعلقة بصلة القيمة بدعامتها المادية والذي اشار بها إلى اهمية الجوهر في مجال المنفعة الاقتصادية اذا ما قورن بما هو مادي، حيث قال " أن أي قانون يرفض ان يرى قيمة في شيء له اهمية سيبقى حتما بمعزل عن الحقيقة"[4].

---

(1) آمال قارة، الجريمة المعلوماتية، رسالة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر، الجزائر، السنة الجامعية 2002/2001، ص77.

(2) علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، بدون رقم طبعة، دار الجامعة الجديدة للنشر، مصر، 1997، ص49.

(3) خثير مسعود، مرجع نفسه ، ص40،ص41.

(4) أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006،ص107.

وفي الاخير نخلص في ظل الآراء الفقهية ان للمعلومات اهمية كبيرة وقيمة اقتصادية عالية مما أدى إلى الاعتراف بوصف المال وانطباقه على المعلومات بناء على ما تم التطرق اليه سابقا.

ثانيا: معارضو إضفاء وصف المال على المعلوماتية

لقد انقسم الفقه المعارض لإضفاء وصف المال على المعلوماتية إلى قسمين فالإتجاه الأول اعتبر المعلومات من قبيل المال المعلوماتي الذي يمكن استغلاله ماليا، والاتجاه الثاني الذي ينظر إلى المعلومات كونها معالجة الكترونيا أو غير معالجة.

1- يرى اصحاب هذا الاتجاه ان المعلومات لا يمكن ان تكون محلا للاعتداء عليها، بحيث أن الفكرة أو المعلومة في حالتها المجردة تكون غير قابلة للتملك او الاستئثار بها وأن تداول هذه الافكار والانتفاع بها هو حق للجميع، وعلى الرغم من الاعتراف لبرامج الكمبيوتر بوصف المال المعلوماتي إلا أنه يبقى استغلالها استغلالاً مالياً كونها مصنفاً فنياً فالاعتداء هنا يقع على حق المؤلف[1].

2- يفرق أصحاب هذا الاتجاه بين المعلومات والبيانات التي تمت معالجتها الكترونيا وبين تلك التي لم تتم معالجتها، بحيث ان هذه الاخيرة يقوم عنصرها الاساسي على الدلالة وليس الدعامة التي تجسدها ماديا وبالتالي لا يمكن ان يقع عليها فعل الاختلاس، اما البيانات والمعلومات المعالجة فإنها تكتسي طابعا ماديا يتمثل في نبضات او اشارات الكترونية ممغنطة يمكن تخزينها على وسائط معينة ونقلها واستغلالها والتصرف فيها بالإضافة إلى امكانية احصاءها كماً ونوعاً، ومن ذلك فإنها تخرج من كونها شيئا معنويا كالأفكار، بل هي شيء له وجود مادي على ارض الواقع[2].

ووفقا لهذا الاتجاه فأنه اذا ما تمت عملية معالجة البيانات والمعلومات فإنها سوف تضفي عليها الطابع المادي وتنقلها من شيئا معنويا إلى شيء مادي محسوس، الامر الذي يؤدي إلى امكانية تطبيق النصوص التقليدية المتعلقة بجرائم الأموال عليها اذا ما تم الاعتداء عليها، وبمفهوم المخالفة اذا لم تتم معالجة هذه المعلومات فإنها لا تصلح لتطبيق النصوص التقليدية عليها لأنها تبقى شيئاً معنويا ولا تكتسي الطابع المادي.

---

[1] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالكمبيوتر وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية، مصر،1995، ص94.

[2] خثير مسعود، مرجع سابق، ص42.

ومن وجهة نظرنا إن عدم اضفاء وصف المال على المعلوماتية يؤدي إلى قصور فرض الحماية الجنائية عليها وحمايتها من كل اعتداء قد يقع عليها لاحقا، وفي ظل عدم الاعتراف بهذه الصفة فإن أي فعل يرتكب عليها لا يمكن متابعة مرتكبه وذلك طبقا لما يقتضيه مبدأ الشرعية الجنائية والذي يعبر عنه بألا جريمة ولا عقوبة الا بنص ، ولتدارك هذا الفراغ التشريعي فإنه من الأرجح إضفاء وصف المال على المعلومات وهذا ما نادى به أصحاب الرأي المؤيد باعتبار المعلومات اموالاً كونها قابلة للاستئثار مما بترتب عنه انتقالها وكذا استغلالها والتصرف فيها، ومن ذلك يتم فرض الحماية الجنائية على المعلومات، وهو الأمر الذي جعلنا نُرَجّح الرأي المؤيد كونه أقرب للواقعية.

الفرع الثاني : مدى اعتبار البرامج مالاً بصدد جرائم الأموال

تشترك جرائم الأموال بصفة عامة بالمحل الذي تقع عليه الجريمة فسنتناول صلاحية البرامج كمحل لجرائم الأموال خاصة جريمة السرقة، النصب، وخيانة الأمانة، فهل تصلح برامج الكمبيوتر كمحل لجرائم الأموال.

أولاً: مدى اعتبار البرامج مالاً بصدد جريمة السرقة

لقد أشار قانون العقوبات الجزائري وكذا العقوبات الفلسطيني سواء في الضفة الغربية أو قطاع غزة من خلال نصوصه على جريمة السرقة بصفة عامة وسنرى إذا ما كان يمكن أن تكون البرامج كمحل لجريمة السرقة؟، تنص المادة 350 من قانون العقوبات الجزائري على : " **كل من اختلس شيئا غير مملوك له يعد سارقا** "[1]، وقد نص قانون العقوبات رقم 16 لسنة 1960 المطبق في الضفة الغربية في المادة 399 على :" **هي أخذ مال الغير المنقول دون رضاه** "[2]، وقد نصت المادة 263 من قانون العقوبات رقم 74 لسنة 1936 المطبق في غزة على: " **كل من أخذ ونقل مالاً قابلاً للسرقة بغير رضا مالكه...**"[3]، من ذلك استقر الفقه و القضاء على أن الأفكار و المعلومات تخرج من النطاق التجريمي لجريمة السرقة كون أن فعل الاختلاس لا يمكن أن يقع إلا على شيء مادي ملموس ومن ذلك نرى أن الأفكار و المعلومات ذو طبيعة معنوية ولا وجود لها

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم، الجريدة الرسمية العدد 48، الجزائر، 1966، المادة 350.
(2) دولة فلسطين، قانون العقوبات رقم 16 لسنة 1960 الأردني المطبق في الضفة الغربية، المادة 399.
(3) دولة فلسطين، قانون العقوبات رقم 74 لسنة 1936 المطبق في قطاع غزة، المادة 263.

ماديا على أرض الواقع و لذلك تخرج من ذلك النطاق و بالتالي لا نتصور بصددها سلطات الحيازة المادية فهي ليست محلا للحقوق و المزايا التي تطالها جريمة السرقة بالعدوان، ومما سبق يتضح لنا أن الأفكار و المعلومات لا يمكن أن تكون محلاً لارتكاب جريمة السرقة عليها إلا في حالة البرامج والبيانات المفرغة على دعامة المادية مما يعطيها الطبيعة الخاصة بالشيء الذي يكون محلاً للاختلاس في جريمة السرقة.

وما يمكن الإشارة إليه أن هذا الاتجاه الفقهي و القضائي في الوقت الذي تبنوا فيه هذا الاتجاه كانت الأشياء المعنوية وقت ذلك لا تتمتع بالقيمة المالية و الاقتصادية العالية ، مما دفع بهم إلى اعتبار محل جريمة السرقة هو الأشياء المادية فقط، ولكن قيمة هذه الأشياء المعنوية بدأت بالتطور واكتساب القيمة الاقتصادية[1]، وبإمعان النظر في المواد 350 من قانون العقوبات الجزائري والتي اشترطت أن يكون شيئا، والقانون رقم 16 لسنة 1960 المطبق في الضفة لا سيما المادة 399 اشترط مالا منقولا، وكذا المادة 263من القانون رقم 74 لسنة 1936 المطبق في غزة والتي اشترطت مالاً قابلاً للسرقة، من ذلك نرى بأن كلا التشريعين لم يشترطا صراحة أن يكون الشيء محل الاختلاس هو شيئا ماديا حيث أن المادتين لم يذكرا مصطلح الأشياء المادية أو الأموال المادية ، لذلك يمكن أن تقع جريمة السرقة على هاته المعلومات و الأفكار إذا ما تم الاعتداء عليه.

وهذا ما دفع القضاء والفقه إلى تأييد ذلك القول و ذلك عند إقرارهم لاختلاس التيار الكهربائي على الرغم من كون طبيعته غير مادية إلا أن جريمة السرقة ترتكب عليه ، وإن كان البعض لا يذهب إلى اعتبارها شيئا معنويا و يطبق عليها مبدأ تجريم الاستيلاء على الطاقة ، كما ذهب جانب من الفقه أن كل قوة أو طاقة يمكن أن يسيطر عليها الانسان كالطاقة النووية مثلا أو التيار الكهربائي فإنه يمكن أن تقع عليه جريمة السرقة وقياسا على ذلك فإن هذه البرامج والمعلومات تشكل طاقة ذهنية على اعتبار أنها تقبل التملك من خلال الاسلاك التي تمر بها[2].

وبالرجوع إلى نصوص جريمة السرقة نجدها تقبل تفسير ارتكاب هذه الجريمة على الأشياء المعنوية، فالبرامج لا يمكن نقلها إلا بموافقة حائزها بحيث هو الوحيد الذي يمكنه إطلاقها و حسبها وفق مشيئته، بالإضافة إلى ان النصوص المتعلقة بجريمة السرقة في كلا التشريعين الجزائري

(1) خثير مسعود، مرجع سابق، ص43.
(2) آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، بدون رقم طبعة، دار هومة، الجزائر،2006،ص19.

والفلسطيني يمكن اسقاط تعريف المال على محل الجريمة وهو كل شيء غير خارج عن التعامل بحكم طبيعته او بحكم القانون، ومن ذلك يمكن القول بأن جريمة السرقة يمكن أن تقع على الأشياء غير المادية[1].

ثانياً: مدى اعتبار البرامج مالاً بصدد جريمة النصب

تصلح البرامج أن تكون محلا لجريمة النصب أو الاحتيال بحيث أن النصوص المتعلقة بجريمة النصب جاءت عامة ولم تحدد طبيعة الشيء محل الجريمة ، و بمفهوم المخالفة يمكن أن تقع جريمة النصب على هاته البرامج كونها شيئا معنويا، وبإمعان النظر في المادة 372 من قانون العقوبات الجزائري والتي تنص على : " **كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو ابراء من التزامات أو إلى الحصول عن أي منها أو شرع في ذلك و كان ذلك بالاحتيال** ... "[2]، و بالرجوع إلى المادة 417 من القانون رقم 16 لسنة 1960 المطبق في الضفة الغربية : " **كل من حمل الغير على تسليمه مالا منقولا أو غير منقول أو أسنادا تتضمن تعهدا أو ابراء فاستولى عليها احتيالا** ... "[3]، وبالنظر إلى احكام قانون العقوبات رقم 74 لسنة 1936 لا سيما المادة 301 والتي تنص على " **كل من حصل من شخص اخر على شيء قابل للسرقة أو حمل شخصا على أن يسلم شيئا قابلا للسرقة إلى شخص اخر متوسلا إلى ذلك بأي وسيلة من وسائل النصب...**"[4]، ومن ذلك يتبين عمومية كلا النصوص السابقة ومنه امكانية أن تقع جريمة النصب على البرامج كون أن النصوص السابقة لم تحدد الطبيعة المادية التي تكون محل لارتكاب جريمة النصب، وهو ذات الأمر في جريمة السرقة بحيث أن يمكن أن تكون البرامج محلا لارتكاب جريمة السرقة باعتبارها أموالا، وهو الأمر الذي يجعل من تطبيق النصوص المتعلقة بجريمة النصب ممكنا بالنظر لعمومية محل الجريمة في تلك النصوص.

---

(1) آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، مرجع سابق،ص20.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، المادة 372.

(3) دولة فلسطين، قانون العقوبات رقم 16 لسنة 1960 مصدر سابق، المادة 417.

(4) دولة فلسطين، قانون العقوبات رقم 74 لسنة 1936 مصدر سابق، المادة 301.

ثالثاً: مدى اعتبار البرامج مالاً بصدد جريمة خيانة الأمانة

من جرائم الأموال جريمة خيانة الأمانة و التي نص عليها المشرع الجزائري في المادة 376 والتي تنص على: " **كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو ابراء ...**" [1]، كما جاءت المادة 422 من قانون العقوبات رقم 16 لسنة 1960 المطبق في الضفة الغربية تنص على ما يلي: " **كل من سلم إليه ... ما كان لغيره من أموال و نقود و أشياء و أي سند يتضمن تعهدا أو ابراء و بالجملة كل من وجد في يده شيء من هذا القبيل** ... "[2]، ومن خلال المواد سالفة الذكر يتبين بأنه لم يتم تحديد الطبيعة المادية للشيء محل جريمة خيانة الأمانة، و نستنتج بأن الأشياء المعنوية و التي من الممكن أن تتمثل بالبرامج فتكون محلاً لارتكاب جريمة خيانة الأمانة أو جريمة إساءة الائتمان ، كون أن البرامج يمكن أن يتم ادراجها ضمن مصطلح البضائع المذكور في المادة 376 وأيضا يمكن إدراجها ضمن مصطلح الأموال المذكور في المادة 422 ، لأن هذه البرامج تتمتع بقيمة اقتصادية عالية و كذلك يسمح لها بالتداول و اجراء عقود بشأنها.

والملاحظ أننا نجد عكس ذلك بالنسبة لقانون العقوبات رقم 74 لسنة1936 فيما يتعلق بجريمة اساءة الائتمان لا سيما المادة 312 [3]، وبإمعان النظر في هذه المادة نجد بأنه يتعذر تطبيقها اذا ما انصبت خيانة الامانة على برامج الكمبيوتر، كون ان المادة حددت شخص الجاني بالأمين على الاوقاف أو الوصايا، ومنه يتضح لنا بأن محل هذه الجريمة هو شيء مادي كالوقف والذي هو حبس العين، ما يفهم منه ان هذا النص الكلاسيكي لا يمكن ان يجرم فعل خيانة الامانة الذي يقع على المعلومات كبرامج الكمبيوتر.

الفرع الثالث: النشاط الاجرامي لجرائم الأموال والمعلوماتية

تتمحور الدراسة في هذا الفرع حول مدى خضوع المعلوماتية متمثلة ببرامج الكمبيوتر للنشاط الاجرامي أو الفعل الذي يتحقق به جرائم الأموال لا سيما جريمة السرقة، النصب، وخيانة الامانة

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، المادة 376.

[2] دولة فلسطين، قانون العقوبات رقم 16 لسنة 1960 مصدر سابق، المادة422.

[3] دولة فلسطين، قانون العقوبات رقم 74 لسنة 1936 مصدر سابق، انظر المادة 312.

وسنخوض أولا في امكانية خضوع برامج الحاسب الالي للسلوك المجرم في جريمة السرقة، ثم على نفس النحو سنتناول امكانية خضوع برامج الحاسب الالي في جريمة النصب وخيانة الامانة.

أولاً: مدى خضوع برامج الحاسب الالي لفعل الاختلاس في جريمة السرقة

يتمثل السلوك المجرم في جريمة السرقة بفعل الاختلاس، وهو الاستيلاء على الحيازة الكاملة للشيء دون رضا مالكه، ويتحقق الاستيلاء إما بنزع الشيء أو بالاستيلاء عليه بعد سبق تسليم اليد العارضة، ومن ذلك يفقد مالكه سيطرته أو حيازته على الشيء ،ويفترض الاستيلاء إخراج الشيء الذي تم الاستيلاء عليه من ذمة صاحبه إلى ذمة الشخص الذي استولى عليه، بمعنى اخر إفراغ ذمة وإشغال ذمة اخرى بحيث لا يوجد مجال للتزاحم بين الذمتين في الاستيلاء على الشيء[1].

وبإمعان النظر في مفهوم فعل الاختلاس لجريمة السرقة نجد بأن هناك عدة عقبات عند تطبيق هذا المفهوم عند سرقة برامج الكمبيوتر وتتمثل تلك العقبات فيما يلي:

1- عند وقوع فعل الاختلاس على برامج الكمبيوتر فإن هذه البرامج لا تنتقل بصفة كلية من ذمة مالكها او حائزها إلى ذمة المستولي عليها، وذلك لأن تلك البرامج لا تخرج من ذمة صاحبها وتبقى تحت سيطرته دون ادنى انتقاص منها، ولكنه يفقد ميزة الاستئثار بها[2]، بمعنى اخر أن البرامج تبقى في ذمة صاحبها ولكن تنتقل إلى شخص اخر كنسخة عنها وليس اختلاسها بمعنى انتقالها بصفة كليه من حيازة صاحبها ودخولها في حيازة من استولى عليها.

2- كما يعتبر من العقبات اختلاس البرامج عن طريق انتقال المعلومة من ذهن إلى ذهن او من ذاكرة إلى ذاكرة ، وهو ما يعرف بالالتقاط الذهني عن طريق السمع أو البصر.

3- واخيرا أن فعل الاختلاس يقع على الأشياء ذات الطبيعة المادية، فكيف يمكن ان يقع على المعلومات التي تحويها البرامج؟ وهذا بحد ذاته يعتبر عقبة عند تطبيق مفهوم فعل الاختلاس على سرقة البرامج المعلوماتية[3].

وفي هذا الصدد اثيرت مشكلة خضوع برامج الكمبيوتر لفعل الاختلاس امام القضاء الفرنسي، والذي حاول التصدي لهذه الجرائم من خلال تقديم حلولا عملية يحاول الفقه من خلالها الوصول إلى التأصيل النظري لتجاوز هذه العقبات، وانقسم الفقه حول هذه المسألة، فمنهم من يرى

(1) علي عبد القادر القهوجي، مرجع سابق، ص60،ص61.
(2) امال قارة، مرجع سابق،ص91.
(3) علي عبد القادر القهوجي، مرجع سابق، ص61.

انها تستعصى عن الحل ومنهم من يرى أن حلها أمرا ميسورا وليس بالأمر المستعصي عن الحل[1]، وفي سياق متصل اصدر القضاء الفرنسي عدة أحكام نستنتج منها أن فعل الاختلاس يقع على المعلومات باعتبارها أموالاً معنوية ومن ذلك يمكن أن تقع على برامج الكمبيوتر فعل الاختلاس والذي يمثل النشاط الاجرامي لجريمة السرقة[2].

(1) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، بدون رقم طبعة، منشورات الحلبي الحقوقية، لبنان، 2003، ص149-ص151.

(2) أنظر الأحكام الصادرة عن القضاء الفرنسي في قضايا logabax، Heberteau، Antonioli .

انقسم الفقه إلى قسمين بين مؤيد ومعارض لخضوع فعل الاختلاس على برامج الحاسب الالي وهو ما سنفصل فيه على النحو الآتي:

أ- مؤيدو صلاحية المعلومة للاختلاس.

يؤسس جانب من الفقه رأيه من نقطة رئيسية وهي أن طبيعة الشيء المختلس تؤدي إلى اختلاف الطريقة التي يتبعها الجاني للقيام بالسلوك المجرم الذي يتحقق معه الاختلاس، وهكذا يختلف الاسلوب الذي ينفذ به النشاط الاجرامي باختلاف الشيء الذي يقع عليه فعل الاختلاس من حيث طبيعته او حجمه أو وزنه أو مقاومته أو وظيفته أو قيمته، وهو ما اكدت عليه محكمة النقض الفرنسية.

لذلك فإن سرقة شيء مادي تختلف عن سرقة الأشياء المعنوية، بحيث أن الأشياء المادية تحتاج إلى نشاط مادي لاختلاسها، الا أن الامر ليس مثله دائماً عند سرقة شيئا معنويا، فهذه الأخيرة يمكن اختلاسها عن طريق اختلاس الدعامة التي تحويها، ويمكن أيضا اختلاسها مستقلة عن دعامتها وذلك من خلال الالتقاط الذهني للمعلومات عن طريق السمع او البصر وهذا دون أن يكون هناك نشاطا ماديا ملموساً[1].

وما يعاب على هذا القول أنه أذا قام أحد الاشخاص بحفظ ما في كتاب أثناء قراءته دون علم ورضا صاحبه تكون جريمة السرقة قائمة في حقه، لذلك فإن هذا المنطق غير سليم قانونا كون أن القانون الجنائي لا يعاقب على الافكار مهما كانت جسامتها، ولتفادي هذا العيب القانوني ذهب اصحاب هذا الاتجاه إلى ان اختلاس المعلومة يكون بإتيان نشاط مادي، ويتمثل هذا النشاط بالقيام بالنسخ أو التصوير التي من خلالها يتم انتقال المعلومة من الاصل إلى الصورة، أما بالنسبة للمعلومة التي يتم التقاطها ذهنيا فأن فعل الاخلاس لا يقوم بها الا إذا تم وضعها على دعامة مادية الامر الذي يجعل منها قابلة للانتقال من ذمة إلى ذمة أخرى.

يرى انصار هذا الرأي بأن اشتراط مادية النشاط الاجرامي الذي يتحقق به فعل الاختلاس، يرجع السبب في ذلك إلى طبيعة الأشياء التي يقع عليها النشاط الاجرامي، بحيث أن فكرة التسامح بالنسبة لأحد العناصر المكونة للجريمة، يجب أن يقابله تشدد في العناصر الاخرى كالركن المعنوي لجريمة السرقة[2].

---

(1) آمال قارة، مرجع سابق، ص93.

(2) امال قارة، مرجع نفسه ،ص92-ص94.

وهذا ما يبرر اشتراط مادية النشاط الاجرامي عند اختلاس المعلومات، وذلك نظراً للموافقة على وقوع فعل الاختلاس على شيء معنوي خلافا لما هو مستقر عليه في الماضي، وتبعا لذلك يجب أن يكون هناك تشدد في طبيعة الأخذ أو الاختلاس بحد ذاته، فالقول بضرورة تحققه بنشاط مادي وتتحقق هذه المادية عند إفراغ المعلومات على دعامة مادية أياً كانت طبيعتها أو هيئتها، وهو ما يؤكد على ان الاستيلاء على الشيء يختلف باختلاف طبيعة الشيء، فأخذ شيء غير مادي مثل المعلومات لا يكون ماديا الا اذا تم تجسيد هذا الشي على هيئة مادية.

ب- معارضو صلاحية المعلومات للاختلاس.

يرى بعض الفقهاء بأن المعلومات المستقلة عن دعامتها لا تصلح لأن يقع عليها فعل الاختلاس ومنه لا يمكن ارتكاب جريمة السرقة على المعلومات التي تكون مستقلة عن الدعامة المادية، انصار هذا الاتجاه لم يتفقوا على رأي واحد عند تفسيرهم لأحكام محكمة النقض الفرنسية المشار إليها سابقاً، فكل فئة تمتلك رؤية خاصة في تفسير تلك الأحكام على النحو الآتي:

– ذهب الرأي الأول إلى القول بأن السرقة قد وقعت على الأصل، بمعنى أن الاستيلاء وقع على الاصل لمدة زمنية كافية لتصويرها[1]، أي أن الجاني استولى على المعلومات الاصلية لمدة زمنية معينة وهي المدة التي كانت تلزمه لنسخ أو تصوير تلك المعلومات فالسرقة هنا هي سرقة استعمال لهذا الأصل حتى ولو كان هذا الاستيلاء استمر لفترة زمنية قصيرة.

صلاحية المعلومات للاختلاس ينكرها البعض، ولذلك تبعا لكونها تكتسب ولا تُؤخَذ، ذلك أنها تظل على حالها ولو اكتسبها الغير، كما أن حصول الغير عليها ليس من شأنه أن يحرم صاحبها منها وإنما يشارك صاحبها فيها فقط [2].

– أما الرأي الثاني، فهو يرى بأن فعل الاختلاس يقع على الالة وليس على الأصل، وأن تأصيلها بنظرهم لا يخرج عن كونه سرقة لوقت الآلة "Vol du temps machine" ، وفعل الاختلاس بنظر أصحاب هذا الاتجاه يقع على وقت آلة الحاسوب بحد ذاتها، وأن هذا الفعل يتمثل في الاستيلاء عليها ولو لوقت قصير جداً، هو الوقت اللازم لنسخ صور البرامج أو المعلومات الأصلية من خلالها، ونرى بأن هذا الرأي

(1) علي عبدالقادر القهوجي، مرجع سابق،ص69.
(2) خثير مسعود، مرجع سابق، ص54.

شاطر سابقه من حيث اعتبار الحالة سرقة استعمال، إلا أن الاختلاف بينهما يتعلق بمحل الاختلاس فالرأي السابق يرى الاصل محلاً للاختلاس أما الثاني فيرى الماكينة "الآلة" هي محل الاختلاس.

كلا الاتجاهين يصطدم بعقبة واحدة وتتمثل في أنه عندما يتم الحصول على صورة عن المعلومات أو البرنامج دون الاستيلاء على الأصل أو الماكينة عن طريق استخدام طرفية تتصل بالحاسب المركزي سلكياً او لاسلكياً فهنا لا يتم الاستيلاء على الاصل ولا على الالة بحد ذاتها، وأمام هذه العقبة قال أصحاب الرأي المعارض بأن السرقة هنا تقع على التيار الكهربائي اللازم لاستخدام الصورة من خلال الومضات والاشعاعات التي يترتب عنها فنيا استخراج نسخة عن الاصل، إلا أن هذا الرأي لا يرى في ذلك حلاً للمشكلة بحيث أن التيار الكهربائي يكاد لا يذكر مقارنة مع سرقة التيار الكهربائي[1].

غير أننا إذا تفحصنا قانون العقوبات الجزائري نرى بأن المشرع لم ينص صراحة من خلال نصوص جريمة السرقة على سرقة المعلومات، والأمر سيّان بالنسبة للتشريع الفلسطيني سواءً في الضفة الغربية أو في قطاع غزة، لذلك فإن المخرج الوحيد من هذه الدوامة الفقهية حول مدى قابلية برامج الكمبيوتر لتطبيق فعل الاختلاس عليها هو اقتراح تعديل لقوانين العقوبات بالنسبة لكلا المشرعين الجزائري والفلسطيني، والنص صراحةً على سرقة المعلومات من خلال نصوص جريمة السرقة وذلك لمواجهة هذه الظاهرة الحديثة والتي تعيش متطفلة على نواقص وثغرات القانون.

ثانيا: مدى خضوع المعلومات للنشاط الاجرامي في جريمة النصب.

يتمثل النشاط الاجرامي في جريمة النصب بفعل الاحتيال أو التدليس الجنائي الذي يمارسه الجاني على الضحية، وفعل الاحتيال لم يأتِ المشرع الجزائري في المادة 372 وكذا قانون العقوبات المطبق في الضفة الغربية لاسيما المادة 417 منه بتعريف له وعرّفه الفقه بأنه " كل تظاهر أو إيحاء يكون صالحاً لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة النصب هو من جازت عليه حيلة الجاني فانخدع بها وسلمه ماله"[2].

والملاحظ أنّ قانون العقوبات المطبق في قطاع غزة قد عرّف فعل الاحتيال في المادة 300 منه بأنه" **كل بيان أدى باللفظ أو بالكتابة أو استنتج من طريقة السلوك عن أمر واقعي ماضٍ أو حاضر، وهو كاذب في حقيقته يعتبر نصباً وغشاً إذا كان الشخص الذي أداه يعلم بأنه كاذب.**"

(1) علي عبد القادر القهوجي، مرجع سابق، ص70،ص71.
(2) عفيفي كامل عفيفي، مرجع سابق، ص166.

ووسائل الاحتيال حددها المشرع الجزائري في المادة 372 على سبيل الحصر وهو ما سار إليه قانون العقوبات المطبق في الضفة الغربية لا سيما المادة 417، وتتمثل هذه الوسائل فيما يلي:

1. الاسم الكاذب: وهي أن يقوم الجاني باستعمال اسم ليس اسمه وذلك بهدف ايقاع الجاني في الغلط.
2. الصفة الكاذبة أو غير الصحيحة : وهي أن يضفي إلى نفسه صفةً معينة لا تتوفر في الجاني من أجل ايقاع المجني عليه بالغلط من اجل تسليمه للمال.
3. استعمال الطرق الاحتيالية: وهي ان يقوم الجاني بالادعاء الكاذب المدعم بالمظاهر الخارجية من أجل تدعيم موقفه حتى يقوم بإيهام المجني عليه، ويقوم هذا الأخير بتسليمه للمال.

إلا أنه بالرجوع إلى أحكام قانون العقوبات المطبق في قطاع غزة نجد بأنه لم ينص على الوسائل الاحتيالية وجعلها تخضع للسلطة التقديرية واكتفى بذكر الوسائل الاحتيالية أو الغش، ومن ذلك نرجع لما هو متعارف عليه فقهياً فتخضع للوسائل سالفة الذكر.

يتمثل أساس جريمة النصب في الاستيلاء على المال المنقول المملوك للغير بنية تملكه، ويكون ذلك برضاء من المجني عليه الذي وقع في أحد وسائل الاحتيال أو الوسائل الاحتيالية التي مارسها عليه وأدت به إلى تسليم ماله للجاني، فإذا قام الجاني بممارسة الاحتيال على المجني عليه من أجل تسليمه دعامة مادية تحتوي على معلومات فإنه تقع جريمة النصب ويمكن تطبيق النصوص المتعلقة بجريمة النصب عليها، فالنشاط الاجرامي لجريمة النصب والمتمثل في الاحتيال ثار حوله جدلاً فقهيا، من حيث إمكانية وقوع فعل الاحتيال على المعلومات الموجودة في الكمبيوتر، انقسم الفقه حول هذه المسألة إلى 3 اتجاهات[1]:

أ- يرى أنصار هذا الاتجاه عدم امكانية وقوع فعل الاختلاس على الحاسب الالي وايقاعه في الغلط، وبالتالي لا تتوافر جريمة النصب في حق من ارتكب هذا الفعل، ويبررون رأيهم بالقول بأنه يجب لكي تتوافر جريمة النصب أن يكون الجاني والمجني عليه أشخاصاً طبيعيين وبالتالي فهو متصور خداع الشخص المكلف بمراقبة البيانات أو مراجعتها أو فحصها[2].

هناك من يبرر هذا الرأي بأنه يشترط لتوافر جريمة النصب أن يتم التسليم من طرف المجني عليه والاستلام من طرف الجاني لكي تتحقق الجريمة، ولو افترضنا أنه تم التسليم بالقول فإن تلك المعلومات

(1) خثير مسعود، مرجع سابق، ص56.
(2) عفيفي كامل عفيفي، مرجع سابق، ص169.

تبقى في حوزة صاحبها وبالتالي فإنه لا يفقد السيطرة عليها وحيازتها وهو أمر إن كان يتفق وطبيعة المعلومات والبرامج، إلا أنه لا يتفق وطبيعة النشاط الاجرامي لجريمة النصب، وهذا يعني أنه لا تصلح البرامج للخضوع للنشاط الاجرامي لجريمة النصب، ومن الدول التي تساند هذا الرأي لوكسمبورغ، مصر، ألمانيا، الدنمارك، فنلندا، اليابان، النرويج، وإيطاليا[1].

ب- يوسع أنصار هذا الاتجاه من النصوص المتعلقة بالعقاب على جريمة النصب ويمكن تطبيق هذه النصوص على النصب المعلوماتي، بحيث تدخل المشرع الانجليزي سنة 1983، واعتبر خداع الالة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يتوجب المعاقبة عليه، ومن ذلك فإنه يمكن تطبيق النصوص المتعلقة بجريمة النصب على ذلك الغش او الاحتيال بطرق معلوماتية وتتبناه الدول الانجلوساكسونية ومنها بريطانيا واستراليا وكندا، وهو اتجاه يوسع من النصوص المتعلقة بالعقاب على جريمة النصب[2].

ج- تُطَبقه الولايات المتحدة الامريكية، حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الاجرامي لغرض الغش على حالات النصب، وعلى المستوى الفيدرالي فقد صدر قانون سنة 1984 يعاقب على "**الولوج غير المشروع أو المصطنع في الحاسب الالي**"، بحيث جاء هذا النص ليعاقب كل من لم يأذن له بالدخول أو من كان مسموحاً له بالدخول إلى الحاسب الالي وقام بأفعال لا يشملها الاذن الممنوح له، وقام الشخص باستعمال او اتلاف او افشاء تلك المعلومات المخزنة على الحاسب الالي وكانت تلك الافعال سبباً في عدم قيام الحاسب الالي بوظيفته، فإنه يمكن إعمال النصوص المتعلقة بالنصب المعلوماتي[3].

وفي الأخير نستعرض موقف المشرعين الجزائري والفلسطيني من تلك الآراء سالفة الذكر، بحيث نرى أن المشرع الجزائري قد حذا حذو المشرع الفرنسي، ومنه يمكن خضوع المعلومات للنشاط الاجرامي لجريمة النصب اذا ما كانت تلك المعلومات مثبتة على دعامة مادية، ففي حال ما إذا كان النقل للمعلومات نقلاً شفويا فهنا لا يوجد فعل مادي يجسم الجريمة ومنه لا يمكن إخضاع المعلومات للنشاط الاجرامي لجريمة النصب، أما المشرع الفلسطيني فأتاح إمكانية تطبيق نصوص جريمة النصب اذا ما ارتكب الجاني فعل الاحتيال للتوصل إلى معلومات ما، بحيث تعتمد النيابة العامة على تلك النصوص لتأسيس دعواها عند وقوع جريمة النصب، ففي الضفة الغربية وقطاع غزة نجد الأمر سيّان بينهما.

(1) آمال قارة، مرجع سابق، ص99.
(2) نبيل صقر، الوسيط في شرح جرائم الأموال، بدون رقم طبعة، دار الهدى، الجزائر، 2012، ص241،ص242.
(3) نبيل صقر، مرجع نفسه ، ص242.

ثالثاً: مدى خضوع المعلومات للنشاط الاجرامي لجريمة خيانة الأمانة.

يتمحور أساس النشاط الاجرامي في جريمة خيانة الأمانة في تسليم المال بناءً على عقد من عقود الأمانة وقيام الأمين باختلاس أو تبديد ما أؤتمن عليه، وذلك من خلال الاستيلاء على الحيازة الكاملة للمال المسلم له على سبيل الأمانة بنية التمليك، أو من خلال التصرف فيه كمنحه لشخص آخر، وما هو متفق عليه في حال تسليم المعلومات على دعامة مادية كالأشرطة أو الأقراص المدمجة ويقوم الأمين بنسخ تلك المعلومات أو تصويرها متجاوزاً الاتفاق الذي بينه وبين صاحب المعلومات أو البرنامج[1] فإنه بذلك يقوم باستنزاف القيمة المادية لتلك البرامج أو المعلومات فيتحقق بذلك فعل الاختلاس، أو من خلال إفشاء المعلومات الموجودة على تلك الدعامة لشخص آخر بقصد الاضرار بصاحب البرنامج أو المعلومات فإن جريمة خيانة الأمانة تكون قائمة، ويعتبر ذلك السلوك مشكلاً للركن المادي لجريمة خيانة الأمانة[2].

لتفنيد إمكانية تطبيق النصوص المتعلقة بجريمة خيانة الأمانة، نستعرض المادة 376 من قانون العقوبات الجزائري والتي نصت على ما يلي: " **كل من اختلس أو بدد بسوء نية أوراقاً تجارية أو نقودا أو بضائع أو مخالصات أو أية محررات أخرى تثبت التزاما أو ابراء ... إضرارا بمالكيها...**"[3]، بإمعان النظر في نص المادة نجد بأن فعل الاختلاس أو التبديد قد يرد على البرامج المثبتة على دعامة مادية إذا ما اعتبرناها من قبيل البضائع والتي تعرف على انها كل ما هو من صنع الطبيعة كالثمار أو من صنع الانسان كالمخططات الهندسية، فمنه يمكن أن ترتكب على البرامج النشاط الاجرامي المتعلق بخيانة الامانة، إلا أن الامر عكس ذلك أذا ما كانت تلك المعلومات أو البرامج مستقلة عن الدعامة مادية فمن الصعوبة بمكان القول بإمكانية خضوعها للنشاط الاجرامي لجريمة خيانة الأمانة.

أما التشريع الفلسطيني فبالرجوع إلى أحكام قانون العقوبات المطبق بالضفة الغربية لا سيما المادة 422 والمتعلقة بإساءة الائتمان نجدها تنص على ما يلي: " **كل من سلم إليه على سبيل ... فكتمه أو بدله أو تصرف به تصرف المالك أو استهلكه أو أقدم على أي فعل يعد تعدياً أو امتنع عن تسليمه لمن يلزم تسليمه إليه،...**"[4]، وفي هذا الصدد أيضا نجد أن قانون العقوبات المطبق في غزة عند نصه على

---

(1) علي عبد القادر القهوجي، مرجع سابق، ص73،ص74.
(2) خثير مسعود، مرجع سابق، ص60،ص61.
(3) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، المادة 376.
(4) دولة فلسطين، قانون العقوبات رقم 16 لسنة 1960 مصدر سابق، المادة 422.

إساءة الائتمان في المادة 312 قد حصر الجاني ومحل الجريمة فالجاني هو الأمين على الاوقاف ومحل الجريمة هو كل ما تم وقفه للجهات العامة أو الخاصة ومنه يتعذر تطبيق هذا النص على هذا النوع من الجرائم، فيتضح لنا جلياً الفرق بين القانون المطبق بالضفة الغربية عن ذلك المطبق في غزة فالمادة 422 يمكن أن يقع السلوك المجرم المنصوص عليه فيها على المعلومات أو البرامج التي تكون مثبتة على دعامة مادية أو تم إفشاء تلك المعلومات لفائدة شخص آخر، إلا أنه لا يمكن ذلك عند تطبيق المادة 312 المتعلقة بإساءة الائتمان من قانون العقوبات المطبق في غزة.

المطلب الثاني: ضرورة استحداث نصوص جنائية خاصة تعنى بالجريمة المعلوماتية.

نتناول في هذا الصدد كيفية مواجهة الجريمة المعلوماتية والتصدي لها من خلال استحداث المشرع لنصوص خاصة بالجريمة المعلوماتية، من هنا نستعرض تلك المواجهة من خلال التشريعين الجزائري والفلسطيني وسنتعرض لكل منهما في فرع خاص به.

الفرع الأول: استحداث نصوص جنائية خاصة في قانون العقوبات الجزائري.

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الالي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة في الاجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر سنة 2004، المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، وذلك بإضافة القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات المواد من 394 مكرر إلى 394 مكرر 7، ليأتي بعد ذلك تعديل سنة 2016 بموجب القانون رقم 16-02 والذي جاء بالمادة 394 مكرر 8.

وقبل الولوج للجرائم، يجب توضيح معنى نظام المعالجة الالية للمعطيات أو البيانات والذي هو علم قائم بذاته، فإن كلمة معلوماتية هي نتاج دمج كلمة معلومة information وكلمة آلية automatic ومعناها المعالجة الآلية للمعلومة، ويفهم من المعطيات الفكرية المعالجة آلياً هي عمل البرامج والبيانات الموجودة في الكمبيوتر وعلى شبكة الانترنت سواء كانت فنية أو أدبية أو علمية أو تجارية، فهي تعتبر انتاج ذهني لصاحبها، ومنه تفرض عليها الحماية القانونية في مواجهة الانتهاكات جرّاء الدخول غير المشروع في انظمة المعالجة الآلية للمعطيات أو البقاء فيها[1].

[1] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، بدون رقم طبعة، دار الهدى، الجزائر،2011،ص48.

أولاً: جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

نصت عليها المادة 394 مكرر من قانون العقوبات الجزائري[1]، بإمعان النظر في المادة المذكورة نجد بأن الجريمة تحتمل صورتين إحداها بسيطة والأخرى مشددة، بحيث جرم المشرع الجزائري في هذه المادة فعل الدخول بطريقة غير مشروعة إلى المنظومة المعلوماتية، حيث أن اختراق الحاسب الالي لأي سبب كان يعد انتهاكاً للنظام المعلوماتي، وفعل الدخول في نظام الحاسب هو دخول معنوي بالاتصال الفكري مع نظام الحاسب وذلك باستخدام تقنيات متعددة لذلك الغرض، كاستخدام البرامج المتخصصة لاختراق انظمة الحماية الفنية للنظام المعلوماتي، أو عن طريق أبواب تسمى "Ttapdoor" الذي يقصد به ترك فواصل في البرامج اثناء اعدادها والتي تستخدم في إضافة وجه من أوجه التلاعب[2].

أما فعل البقاء فيقصد به التواجد داخل نظام المعالجة الآلية للمعطيات بدون رضا صاحب الحق في النظام، بحيث تكون نية الفاعل البقاء بطريقة غير مشروعة حتى ولو دخل عن طريق الصدفة[3]، وقد يكون الدخول مصرح به من طرف صاحب النظام إلا أنه مشروط بخروجه بعد انقضاء مدة معينة فلا يقوم الجاني بالخروج من نظام المعالجة الآلية بعد انتهاء المدة، فيكون بقاءه غير مشروعاً في هذه الحالة.

نلاحظ بأن المشرع لم يحدد الوسيلة التي ترتكب بها الجريمة سواء فعل الدخول او البقاء، واكتفى المشرع في المادة 394 مكرر ذكر النشاط الاجرامي الذي تتحقق به الجريمة فقط، وتجدر الإشارة إلى أن تحقق فعل الدخول او البقاء يخضع للسلطة التقديرية للقاضي وجوده من عدمه وهذه هي الصورة البسيطة من المادة 394 مكرر/1.

أما الصورة المشددة، المشرع الجزائري شدد في العقوبة وجعلها مضاعفة بنص المادة 394 مكرر من قانون العقوبات إذا ترتب عن الدخول أو البقاء في النظام حذف أو تغيير لمعطيات المنظومة إذ نص في الفقرة الثانية والثالثة من المادة المشار اليها سابقاً على ما يلي :" **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة**"، وتتحقق هذه الصورة بما يلي:

---

(1) ، الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم، مصدر سابق، المادة 394 مكرر.

(2) امال قارة، مرجع سابق، ص42،ص43.

(3) طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة الجزائر1، الجزائر، السنة الجامعية 2012/2011، ص55.

أ. الحذف والتغيير: وهي الحالة التي يقترن بها الدخول او البقاء في منظومة المعالجة الآلية بفعل الحذف والذي يقوم الجاني من خلاله بمسح البيانات والمعلومات المخزنة داخل نظام المعالجة الآلية، اما التغيير فهو يتعلق أساساً بعملية التعديل وتبديل المعلومات الموجودة على نظام المعالجة الآلية، وقد يكون ذلك الحذف أو التغيير كلي أو جزئي، وترتفع العقوبة إلى الحبس من 6 اشهر إلى 2 سنتين والغرامة من 100.000دج إلى 400.000 دج[1].

ب. التخريب: وهو إفساد منظومة المعالجة القانونية على نحو يجعل منها غير قابلة للعمل مرة أخرى، وترتفع به العقوبة إلى الحبس من 6 أشهر إلى 3 سنوات والغرامة من 50.000دج إلى 150.000 دج، وتكون هذه الظروف قائمة سواء كان الخطأ عمدياً أو غير عمدي، وبالنظر إلى هذه لظروف نجد بأنها ظروفاً مادية بحيث لا يمكن للجاني أن ينفيها عن نفسه إلا إذا أثبت وقوع قوة قاهرة أو حادث مفاجئ.

ثانياً: جرائم الاعتداءات العمدية على سلامة المعطيات.

وسنقسم هذه الاعتداءات إلى قسمين :الاعتداءات العمدية على المعطيات داخل النظام الإتلاف المعلوماتي، والاعتداءات العمدية على المعطيات خارج النظام.

1- الاعتداءات العمدية على المعطيات داخل نظام المعالجة الآلية الإتلاف المعلوماتي.

نصت على هذا النوع من الجرائم المادة 394 مكرر1 من قانون العقوبات الجزائري، والنشاط الإجرامي المكون لجريمة الاعتداء العمدي على المعطيات داخل النظام ينحصر هذه الأفعال ب 3 صور وهي: الإدخال، التعديل والإزالة، ومن هنا يمكن القول أن النشاط الاجرامي ينصب على المعطيات أي المعلومات المعالجة آلياً، كما أن المعلومات محل الجريمة هي تلك المعلومات التي تكون داخل نظام المعالجة وليس خارجها، وبناء عليه فأن الجريمة لا تقع إذا انصب النشا الاجرامي على المعلومات خارج نظام المعالجة الآلية، وسنبين فيما يلي صور السلوك المجرم كلٌ بحسب مدلوله[2]:

أ. فعل الإدخال: هو إدراج برنامج ما، والذي هو عبارة عن تعليمات بلغة ما توجه إلى كيان الحاسوب بغرض الوصول إلى نتيجة معينة والتي تشكل هدف الجاني جرّاء ارتكابه لهذه الجريمة، فإن البرنامج الجديد قد يكون وهمياً يهدف إلى التمويه والتضليل وتغيير الحقيقة وتعتبر مرحلة إدخال البيانات او

(1) زبيحة زيدان، مرجع سابق، ص51.
(2) خثير مسعود، مرجع سابق، ص123.

البرامج او المعطيات الجديدة، أهم المراحل في الجريمة الالكترونية، بحيث انها مرحلة سابقة على مرحلة استغلال المعلومات أو المعطيات كقيام طالب بإدخال علامات جديدة على حسابه الخاص بالجامعة[1].

ب. فعل الإزالة: ونقصد بهذا الفعل قيام المجرم بأفعال تؤدي إلى محو جزء من المعطيات المسجلة داخل نظام المعالجة، أو تحطيم الدعامة التي تعمل على حفظ المعلومات داخل النظام، أو نقل وتخزين جزء من المعطيات إلى منطقة غير خاصة بالذاكرة التي تعمل على استرجاع المعلومات والمعطيات عند استدعائها من النظام.

ج. فعل التعديل: ومعناه تغيير المعطيات والمعلومات الموجودة والمخزنة داخل نظام المعالجة الآلية واستبدالها بمعلومات أخرى، وقد يتحقق ذلك عن طريق برامج لها القدرة على التلاعب في معطيات النظام، كتعديلها باستخدام أساليب معلوماتية خاصة كالقنبلة المعلوماتية، أو برنامج الممحاة، وبرنامج حصان طروادة، وأفعال الإدخال أو الازالة أو التعديل ذكرها المشرع على سبيل الحصر لا المثال من خلال المادة 394 مكرر 1 عند ارتكاب جريمة الاعتداء العمدي على المعطيات داخل النظام أو ما يعرف بالإتلاف المعلوماتي[2].

2- الاعتداءات العمدية على المعطيات خارج نظام المعالجة الآلية.

تناولتها المادة 394 مكرر2 من قانون العقوبات الجزائري[3] مسألة الاعتداءات العمدية خارج النظام، وبإمعان النظر في المادة نجدها تشمل وصفين لهذه الجريمة:

أ. عندما تكون فيه المعطيات وسيلة لارتكاب جريمة من جرائم الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات وتتمثل هذه الأفعال فيما يلي: التصميم، البحث، التجميع، التوفير، النشر والاتجار في المعطيات أو المعلومات التي تمت معالجتها أو مخزنة أو مرسلة والتي تكون موجودة خارج النظام، ونلاحظ بأن المشرع الجزائري يشترط لقيام هذه الجريمة ان تكون المعطيات تم اعدادها خصيصاً لارتكاب جريمة من الجرائم المعلوماتية، على عكس ما ذهب إليه المشرع الفرنسي والذي تقوم بحسبه الجريمة حتى ولو كانت المعطيات موجهة لأي وظائف أخرى غير الاجرام المعلوماتي.

---

(1) زبيحة زيدان، مرجع سابق، ص54.

(2) طرشي نورة، مرجع سابق، ص57،ص58.

(3) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، المادة 394 مكرر2.

ب. تكون فيه المعطيات متحصلة أو ناتجة عن ارتكاب جرائم الاعتداءات الماسة بنظام المعالجة الآلية للمعطيات، وتتحقق بإتيان أحد الأفعال المتمثلة في حيازة أو إفشاء أو نشر أو استعمال ما تم التحصل عليه من جرائم الاعتداء العمدي على نظام المعالجة الآلية للمعطيات[1].

ولتوضيح المفهوم بالأفعال السابقة سنتناولها كما يلي:

- الحيازة: وهي أن يقوم الجاني بحفظ البيانات في حوزته دون إذن أو ترخيص يسمح له بذلك، وفي حقيقة الأمر أن المشرع لم يشترط الإذن هنا كون أن هذه المعلومات تكون قد تم التحصل عليها من خلال الجريمة التي تم ارتكابها.
- الإفشاء والنشر: وهي أن يقوم الجاني ببث ونشر ما تحصّل عليه من الجريمة بأي وسيلة من الوسائل شريطة أن يكون ما قام بنشره وإفشاؤه ناتج عن جريمة من الجرائم التي تم النص عليها في القسم السابع مكرر من قانون العقوبات الجزائري.
- الاستعمال: ويقصد بها أن يقوم مرتكب احدى الجرائم المنصوص عليها في القسم السابع مكرر باستخدام ما قام بالتحصل عليه من الجريمة التي قام بارتكابها.

ثالثاً: الجرائم المرتكبة من طرف مقدم خدمات الإنترنت.

نص المشرع الجزائري على هذا النوع من الجرائم من خلال المادة 394مكرر8، والتي تم استحداثها بموجب التعديل الجديد لقانون العقوبات الجزائري بموجب القانون رقم 16-02 المؤرخ في 19 يونيو 2016[2]، بالرجوع إلى هذه المادة لتعريف مقدم خدمات الانترنت، نرى أن القانون قد أحالنا لتعريفه إلى القانون رقم 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بحيث جاء تعريفه في المادة الثانية الفقرة د على أنه:

---

(1) بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، الجزائر، السنة القضائية 2010-2011، ص14،ص15.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، المادة 394 مكرر8.

1- "أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات،

2- وأي كيان آخر يقوم بمعالجة او تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها"[1].

وحملت المادة 394مكرر8 الصورتين الآتيتين:

1- الامتناع عن التدخل الفوري لسحب المعلومات أو تخزين المحتويات التي يتيح مقدم الخدمات الاطلاع عليها من طرف مستخدميه ، وكذا حالة امتناع مقدم خدمات الانترنت عن جعل الدخول إلى المعلومات غير ممكن، بحيث تكون المعلومات محتواها غير قانوني مما يستلزم جعلها غير متاحة للدخول إليها فيمتنع مقدم خدمات الانترنت عن ذلك، وبهذا التصرف يعتبر مرتكباً للجريمة المنصوص عليها في المادة 394 مكرر8 الفقرة 1.

2- أما الصورة الثانية، فهي تتمثل في امتناع مقدم خدمات الانترنت عن تسخير التقنيات اللازمة التي تساهم في سحب المعلومات أو تخزينها عندما تتعلق بالجرائم المذكورة بالصورة الأولى. تجدر الإشارة إلى أنه إلى جانب العقوبة الجزائية فهناك عقوبات ادارية توقع على مقدم خدمات الانترنت في حالة ارتكابه للجريمة، فعقابه جزائيا لا يحول دون مساءلته إداريا، وهذا ما تم تأكيده بنص المادة 394 مكرر8.

ثالثاً: العقوبات المرصودة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

لقد سار المشرع الجزائري وفقا للنهج الدولي الذي ينادي بعقوبات رادعة في مجال الاجرام المعلوماتي، ويتجلى ذلك عند الرجوع لأحكام القسم السابع مكرر المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، نرى بأن المشرع الجزائري اتبع التدرج الهرمي في إقرار العقوبات الجزائية وذلك تبعا للخطورة الاجرامية التي تنّمُ عنها كل جريمة، بحيث نصَّ على جريمة الدخول أو البقاء بصورتيها البسيطة والمشددة تباعاً باعتبارها الأخف، ثم نصّ على الاعتداءات العمدية الماسة بأنظمة المعالجة الآلية للمعطيات باعتبارها الأشد[2].

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 5 غشت 2009، الجريدة الرسمية العدد47، الجزائر، 2009، ص5، المادة2، انظر الملحق رقم 1.

[2] خثير مسعود، مرجع سابق، ص126.

لقد عاقب المشرع الجزائري على جريمة الدخول او البقاء غير المشروع المنصوص عليها بالمادة 394 مكرر بصورتها البسيطة بالحبس من 3 أشهر إلى سنة واحدة والغرامة من 50.000 دج إلى 200.000 دج، أما إذا ارتكبت جريمة الدخول أو البقاء غير المشروع بصورتها المشددة وذلك وفقاً لما جاء في المادة 394 مكرر/3/2 فإنه ترتفع العقوبة بناءً على ما جاء في الفقرة الثانية من 6 أشهر إلى سنتين والغرامة من 100.000دج إلى 400.000 دج كون الفقرة الثانية جاءت بمصطلح تضاعف العقوبة أي العقوبة المنصوص عليها في الفقرة الأولى الصورة البسيطة، اما اذا ارتكبت الجريمة بناءً على احكام الفقرة الثالثة فإنه نص المشرع صراحة على العقوبة بالحبس من 6 أشهر إلى 3 سنوات والغرامة من 50.000 دج إلى 300.000 دج[1].

أما العقوبات المقررة للاعتداءات العمدية الماسة بالمعطيات داخل نظام المعالجة الآلية المنصوص عليها في المادة 394 مكرر1، فتكون العقوبة الحبس من 6 أشهر إلى 3 سنوات والغرامة من 500.000 دج إلى4.000.000[2].

كذلك العقوبات المقررة للاعتداءات العمدية الماسة بالمعطيات خارج نظام المعالجة الآلية، فقد خصها المشرع طبقاً لنص المادة 394 مكرر2 بعقوبة الحبس من شهرين 2 إلى3 سنوات وبغرامة من 1.000.000 دج إلى10.000.000[3].

وأخيراً عاقب المشرع الجزائري على الجرائم التي يرتكبها مقدموا خدمات الانترنت بالحبس من سنة إلى 3سنوات والغرامة من 200.000 دج إلى 10.000.000، وذلك استناداً لما جاء في المادة 394 مكرر8، ودون الاخلال بالعقوبات الادارية بطبيعة الحال[4].

وتجدر الإشارة إلى تشديد العقوبة بحيث تصبح ضعف العقوبة المقررة للجريمة إذا ما كانت الجرائم سالفة الذكر استهدفت الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام، وإذا كانت هناك عقوبة أشد عند مضاعفة العقوبة الاصلية المقررة فإنه يتم تطبيق العقوبة الأشد، وهذا وفقاً لما جاي في المادة 394 مكرر3[5].

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم ، مصدر سابق، انظر المادة 394 مكرر.
(2) الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، انظر المادة 394 مكرر1.
(3) الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، انظر المادة 394 مكرر2
(4) الجمهورية الجزائرية الديمقارطية الشعبية، المصدر نفسه، انظر المادة 394 مكرر8.
(5) الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، انظر المادة 394 مكرر3.

الملاحظ على العقوبات التي اوردها المشرع الجزائري في قانون العقوبات هي عقوبات متناسبة مع الفعل المجرم، بحيث لم يشدد العقوبة للدرجة التي تؤدي به إلى الابتعاد عن فكرة إصلاح وتأهيل المجرمين، وكذلك راعى المشرع الجزائري تحقيق الردع العام والخاص من خلال تلك العقوبات وهو الهدف من العقاب.

فيما يخص مساءلة الشخص المعنوي، فقد شمله المشرع بالتجريم والعقاب، بحيث يُسأل الشخص المعنوي جزائياً عن هذه الجرائم بصفته فاعلاً أصلياً أو شريكاً أو متدخلاً كما يُسأل عن الجريمة التامة أو الشروع فيها كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه الشرعيين، وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل 5 مرات الشخص الطبيعي، وهذا طبقاً لما جاء في المادة 394 مكرر4[1]، بالإضافة إلى امكانية توقيع العقوبات المنصوص عليها في المادة 18 مكرر من قانون العقوبات الجزائري، إلى جانب العقوبات التكميلية سواء الخاصة بالجريمة المعلوماتية أو المتعلقة بكافة الجرائم.

أما الاشتراك في الجريمة، تناوله المشرع الجزائري في المادة 394 مكرر5 من قانون العقوبات، نجد بأن المشرع الجزائري احتفظ بأصله في احكام المساهمة الجنائية لا سيما اذا تعلق الأمر بالعقوبة، حيث رصد لها نفس العقوبة المقررة للجريمة التامة، كما ان هذا النوع من الجرائم لا يشترط وجود اتفاق حقيقي كون أن النتيجة الإجرامية تبين لنا وجود اتفاق ضمني بين مرتكبي هذا النوع من الجرائم، كما يكون الأمر سيّان سواء كان الاتفاق بين الاشخاص الطبيعية أو المعنوية[2].

وعاقب المشرع الجزائري على الشروع الذي طرح إشكالاً وهو تحديد مرحلة البدء في التنفيذ، بحيث يصعب تحديد هذه المرحلة، لا سيما إذا تعلق الأمر بمحاولة الدخول الاختراق عن بعد وهو الأمر الذي أدى إلى تبني مبدأ المعاقبة على الاتفاق الجنائي بهدف التحضير للجرائم المعلوماتية[3]، وعاقب المشرع الجزائري على الشروع في المادة 394 مكرر7، وذلك بإقرار نفس العقوبة المقررة للجريمة التامة.

---

(1) عاقلي فضيلة، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة في المؤتمر الدولي الرابع عشر: طرابلس 24-25 مارس 2017، لبنان، 2017، ص130.

(2) خثير مسعود، مرجع سابق، ص 129.

(3) آمال قارة، مرجع سابق، ص69.

الفرع الثاني: انعدام النصوص الجنائية في قانون العقوبات الفلسطيني.

الملاحظ أنّ قانون العقوبات رقم 16 لسنة 1960 المطبق في الضفة الغربية وقانون العقوبات رقم 74 لسنة 1936، نجده خلا كلا القانونين من أي نص يجرّم الانتهاكات التي تحدث من خلال اجهزة الكمبيوتر وعليها، والسبب في ذلك هو قدم القانون وغياب المشرع، فالواقع القانوني واحد بالنسبة لفقر القانونين سواء المطبق في غزة أو الضفة الغربية، وهو الأمر الذي يجعل من فرض الحماية الجزائية على المعلوماتية أمراً غير ممكن من خلال هذين القانونين ، إلا فيما يخص تطويع النصوص التقليدية لمحاولة التقليل من حدة وانشار الجريمة الالكترونية، ويتم ذلك من خلال نصوص جريمة السرقة المادة 399، جريمة النصب المادة 417 وجريمة خيانة الأمانة والتي تعرف بإساءة الائتمان المادة422، إلا أن تطويع النصوص التقليدية قد يصطدم بمبدأ الشرعية الجنائية، مع طرح الاشكالات التي تثيرها تلك النصوص عند إعمالها على الجرائم المعلوماتية، وتبقى الجريمة المعلوماتية في التشريع الفلسطيني تتمتع بالإباحة دون التجريم.

تجدر الإشارة إلى وجود مشروع قانون العقوبات الفلسطيني لسنة 2001 والذي تم النص فيه على تجريم الانتهاكات المرتكبة عن طريق الكمبيوتر والانترنت، وذلك من خلال نص المادة 393 من مشروع القانون نصت على ما يلي:"

1- كل من اقتحم بطريق الغش نظاما لمعلومات حاسب آلي خاص بالغير أو بقي فيه يعاقب بالحبس مدة لا تزيد على سنة وبغرامة لا تجاوز ألف دينار أو بإحدى هاتين العقوبتين.
2- وإذا نتج عن ذلك تعطيل تشغيل النظام أو محو المعلومات التي يحتوي عليها أو تعديلها تكون العقوبة الحبس وغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين"[1].

كما جاءت المادة 394 من مشروع القانون ونصت على جريمة إفساد أو عرقلة الحاسب الآلي فنصت على ما يلي: " **كل من عرقل أو أفسد عمدا تشغيل نظام حاسب خاص بالغير أو أدخل أو عدل بطريق الغش معلومات تخالف المعلومات التي تحتوي عليها يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين"[2].**

(1) عبد الكريم خالد الشامي، جرائم الكمبيوتر والانترنت في التشريع الفلسطيني، دنيا الوطن، 2010/05/02، ص15.
(2) عبد الكريم الشامي، مرجع نفسه ، ص15.

نص المشرع من خلال المادة 395 على جريمة التزوير والإضرار بالغير بقولها " **كل من زور إضرارا بالغير وثائق حاسب آلي خاص أو استعمل وثائق مزورة مع علمه بتزويرها يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين**"[1].

ويُحسَب أيضاً للمشرع الفلسطيني أنه أخرج جريمة السرقة من مفهومها التقليدي وأضفى عليها صبغة تجعلها تتماشى مع التطور التكنولوجي الحاصل، بحيث نصت المادة 396 من مشروع القانون على ما يلي : " **كل من سرق معلومات من نظام حاسب آلي خاص بالغير يعاقب بالحبس وبغرامة لا تجاوز ثلاثة آلاف دينار أو بإحدى هاتين العقوبتين**،..."، كما جاء نص المادة 397 من مشروع القانون بالنص على عقوبة الشروع كما يلي: " **يعاقب على الشروع في الجرائم المنصوص عليها في هذا الفصل بذات العقوبة المقررة للجريمة التامة**"[2].

وبإمعان النظر في النصوص التي جاء بها مشروع قانون العقوبات الفلسطيني، نجد بأنه كان على جاهزية تامة للتصدي ومواجهة الجريمة الالكترونية، وذلك بالنظر إلى الأفعال التي جرمها المشرع، فنجد أنها قد حصرت غالبية صور الجريمة المعلوماتية كالدخول والبقاء في نظام الغير، وكذلك تجريم كل أفعال المساس العمدي بالمعطيات والمعلومات من خلال التعديل أو الإزالة أو النشر أو الاستعمال على نحو غير مشروع اذا ما دخل المجرم إلى نظام المعالجة وقام بالتعديل فيه او الازالة، وكذا تجريم النشر أو الاستعمال للمعلومات والتي أساساً تكون متحصلة جرّاء ارتكاب جريمة من الجرائم المعلوماتية التي جاء بها مشروع قانون العقوبات الفلسطيني، إلا أن هذه النصوص نجد بأنها قد أغفلت جانب مهم وهو في حال ما أذا وقع الاعتداء على الدولة أو أحد الاشخاص المعنوية الخاضعة للقانون العام، فلم يشدد العقوبة لكي تكون أكثر ردعاً.

وتجدر الإشارة إلى أن هذا القانون هو مشروع فقط وغير نافذ في المحاكم الفلسطينية، فعند وقوع جريمة تصنف ضمن الجرائم المعلوماتية فلن نجد النص الذي يجرمها، كوننا نرجع لتطبيق الأحكام المنصوص عليها في قانون العقوبات رقم 74 لسنة 1936 المطبق في غزة وكذا قانون العقوبات رقم 16 لسنة 1960 المطبق في الضفة، واللذان لم يشتملا على أي نص يجرم الانتهاكات المرتكبة بواسطة الكمبيوتر والانترنت.

---

[1] عبد الكريم الشامي، مرجع نفسه ، ص15.
[2] عبد الكريم الشامي، مرجع سابق، ص16.

المبحث الثاني

المكافحة الموضوعية للجريمة المعلوماتية في ظل القوانين الخاصة

لا يقتصر فرض الحماية الجنائية على المعلوماتية في قانون العقوبات فقط، بل تمتد صور الحماية إلى أكثر من قانون ، وذلك لضمان حماية متكاملة لنظم المعالجة الآلية للمعلومات، بحيث جاءت نصوص متفرقة لتنص على تجريم بعض الافعال التي تعتبر اعتداء على المعلومات وسلامتها، ومنها: القوانين المكلمة لقانون العقوبات كالقانون المتعلق بالمخدرات والمؤثرات العقلية، القوانين المتعلقة بمكافحة الجرائم المعلوماتية، والقانون المتعلق بالاتصالات السلكية واللاسلكية وذلك في كلا التشريعين الجزائري والفلسطيني.

وفي نفس الصدد طالت يد المشرع لفرض الحماية الجزائية من خلال النصوص المتعلقة بالملكية الفكرية والملكية الصناعية، من حيث مدى اعتبار برامج الحاسب الآلي مصنفاً فنياً وإمكانية فرض الحماية عليه من خلال نصوص الملكية الفكرية، ومن خلال حماية براءات الاختراع في حال وقوع أي اعتداء عليها يتصور وقوعه على برامج الحاسب الآلي وإمكانية حمايتها من خلال تلك النصوص المتعلقة بالملكية الصناعية، وهو ما سنفصل فيه تباعاً بحيث سنتناول في المطلب الأول الحماية الجنائية في القوانين المكملة لقانون العقوبات، وفي المطلب الثاني الحماية الجنائية في النصوص المتعلقة بالملكية الفكرية.

المطلب الأول: الحماية الجنائية في القوانين المكملة لقانون العقوبات

لفرض حماية جنائية شاملة نوعاً ما على شتى أنواع الجرائم، ينص عليها المشرع في قانون العقوبات ثم يخصها بتشريع ليشمل كل الأفعال التي يمكن أن تشكل جريمة من الجرائم التي منحها المشرع قانوناً خاصاً ملحقاً بقانون العقوبات، والأمر هنا يتعلق بكلا التشريعين الجزائري والفلسطيني، لا سيما فيما يخص الجريمة المعلوماتية وتجريم الأفعال التي يمكن أن تشكل جريمة يمكن تصنيفها من قبيل هذا النوع من الجرائم، وسنفصل في كل تشريع على حدى بالشرح والتفصيل من حيث الجرائم الالكترونية المنصوص عليها في القوانين المكملة لقانون العقوبات والأحكام الخاصة بها.

الفرع الأول: الحماية الجنائية في القوانين المكملة لقانون العقوبات الجزائري

تعددت النصوص التي تجرّم الانتهاكات المرتكبة على وسائل تكنولوجيا المعلومات أو تلك التي ترتكب بواسطة الوسائل التكنولوجية، بحيث نصّ كلا المشرعين الجزائري والفلسطيني من خلال القوانين الخاصة الملحقة بقانون العقوبات على تجريم الأفعال التي تعتبر من قبيل الجريمة المعلوماتية.

أولاً: القانون المتعلق بالمخدرات والمؤثرات العقلية.

بالرجوع إلى أحكام القانون رقم 04-18المؤرخ في 25 ديسمبر سنة 2004 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، نلاحظ أن المادة 13 قد اشتملت على سلوكين وهما التسليم والعرض، فالفعل الأول التسليم يعبر عن حالة واقعية يتم بموجبها نقل حيازة الشيء المادي من البائع إلى المشتري، فهذه الصورة تخرج عن نطاق الجرائم المعلوماتية كون أن التسليم للشيء المادي والذي يتمثل في المخدرات لا يراعي خصوصية الجريمة المعلوماتية وطبيعتها الخاصة والتي تقع أساساً على المعلومات[1].

بينما الفعل الثاني والمتمثل في العرض، يقصد به الترويج لبيع المخدرات والمؤثرات العقلية بأي وسيلة من الوسائل ، ونستشف ذلك من خلال نص المادة الذي لم يشترط الوسيلة التي يتم بها الترويج لهذه الممنوعات، لذلك من الممكن أن تكون الوسيلة التي يتم بها العرض عن طريق مواقع الانترنت أو من خلال وسائل التواصل الاجتماعي، وهو ما يعتبر فرضاً للحماية الجزائية على صور الترويج والعرض الالكتروني للمخدرات والمؤثرات العقلية[2].

وعاقب المشرع عليها بعقوبة الحبس من سنتين إلى عشر سنوات وغرامة من 100.000 إلى 500.000 دج، ويضاعف الحد الاقصى للعقوبة إلى 20 سنة حبس وإلى 1.000.000 دج اذا وقع الفعل على قاصر أو معوق او داخل مراكز تعليمية أو تربوية او تكوينية أو داخل المؤسسات العمومية[3].

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 04-18 المؤرخ في 25 ديسمبر 2004 يتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار بها، الجريدة الرسمية العدد 83، 2004، أنظر المادة 13.

[2] الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، انظر المادة 13.

[3] الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، انظر المادة 13.

ثانياً: قانون الوقاية من تبييض الأموال وتمويل الإرهاب.

لقد نص القانون رقم 05-01 المؤرخ في 6 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما في المادتين الثانية والثالثة منه على الأفعال التي تعتبر تبييضاً للأموال وتمويلاً للإرهاب، بحيث يمكن أن ترتكب هذه الجرائم من خلال وسائل التكنولوجيا بشتى صورها، الملاحظ على المادة 2 من القانون رقم 05-01 لا سيما الفقرة الأولى منها[1]، بأنها لم تحدد الوسيلة التي يتم بها تحويل أو نقل العائدات الاجرامية، والتي يكون الغرض منها إخفاء وتمويه الطبيعة الحقيقة لتلك الممتلكات، وكون أن جريمة تبييض الأموال قد تمتد أركانها إلى أكثر من دولة، وبالاشتراك بين مجموعة من الاشخاص بناءً على اتفاق مسبق بينهم، فإنه إذا كانت تلك الممتلكات أموالاً نقدية، فإنه يمكن أن تكون جريمة معلوماتية إذا ما تمت مثلاً عملية تحويل الأموال عن طريق البنوك وذلك من خلال كسر الحواجز الأمنية لنظام البنك من اجل تحويل تلك الأموال إلى الخارج، للحيلولة دون مصادرتها من قبل رجال الضبطية القضائية.

ومنه فإن عملية تحويل الأموال من الممكن أن تكون أحد صور الجريمة المعلوماتية اذا ما تم ارتكابها من خلال الوسائل التكنولوجية الحديثة، وذلك بإقرار المشرع في نص المادة الرابعة الفقرة الأولى والتي جاءت تعرّف لنا الأموال بمفهوم القانون 05-01 والتي تعرّفه بما يلي: "**أي نوع من الأموال المادية أو غير المادية، لا سيما المنقولة أو غير المنقولة التي يحصل عليها بأية وسيلة كانت، والوثائق أو الصكوك القانونية أيا كان شكلها، بما في ذلك الشكل الإلكتروني أو الرقمي،...**".[2]

وقد عاقب المشرع على جريمة تبييض الأموال من خلال المادة 389 مكرر 1، بالحبس من 5 سنوات إلى 10 سنوات والغرامة من 1.000.000 دج إلى 3.000.000 دج، وتشدد العقوبة في حال العود للجريمة، أو باستعمال التسهيلات التي يمنحها ممارسة نشاط مهني، أو في حال ارتكابها في إطار جماعة اجرامية ، فتصبح العقوبة الحبس من 10 إلى 20 سنة والغرامة من 4.000.000 دج إلى 8.000.000 دج، فهي عقوبة رادعة بالشكل الكافي لمكافحة جريمة تبييض الأموال المرتكبة من خلال تكنولوجيا المعلومات.

---

[1] القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الطبعة الاولى، الديوان الوطني للأشغال التربوية، الجزائر،2005،ص5.

[2] القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما ، مرجع سابق، ص6.

أما جريمة تمويل الإرهاب فإنه من المتصور أيضاً ارتكابها من خلال وسائل التكنولوجيا، فتتدرج ضمن الجرائم الالكترونية، ونستنتج ذلك من خلال استقراء نص المادة الثالثة من القانون رقم 05-01 والتي تنص على ما يلي: "**يعتبر مرتكباً لجريمة تمويل الإرهاب ... كل من يقدم أو يجمع او يسير بإرادته، بطريقة مشروعة أو غير مشروعة، بأي وسيلة كانت، بصفة مباشرة أو غير مباشرة...**"[1].

نرى بأن المشرع قد وسّع من طرق تمويل الإرهاب لمحاولة ردع هذا النوع من الجرائم، والتي يتصور ارتكابها من خلال الوسائل الالكترونية، بحيث يستطيع الشخص القيام بالدعوة لتمويل الإرهاب من خلال وسائل التكنولوجيا كإطلاق موقع الكتروني لتمويل الإرهاب أو من خلال استخدام وسائل التواصل الاجتماعي لأجل هذا الغرض، ومنه يتصور أن يكون تمويل الارهاب كأحد صور الجريمة المعلوماتية.

وعاقب المشرع على هذه الجريمة من خلال نص المادة 87 مكرر 4، بالسجن المؤقت من 5 سنوات إلى 10 سنوات والغرامة من 100.000 إلى 500.000 دج. وهي عقوبة تعتبر رادعة إلى حد ما، باعتبارها مرتكبة خارج احكام العود للإجرام.

وتجدر الإشارة بخصوص الجريمة الارهابية أن المشرع الجزائري جاء بالمادة 87 مكرر12 بموجب تعديل 16-02 لسنة 2016 ليجرّم من خلالها تجنيد الاشخاص لصالح الجماعات الارهابية وذلك عن طريق استخدام الوسائل التكنولوجية ، ومنه نرى أن المشرع قد أقرّ صراحة ارتكاب الجريمة الارهابية كأحد صور الجريمة المعلوماتية، وعاقب عليها المشرع بنفس العقوبة لجريمة تمويل الارهاب.

ثالثاً: قانون البريد والمواصلات السلكية واللاسلكية.

جاء القانون 2000-03 المؤرخ في 5 غشت سنة 2000 بالقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ليشتمل على عدة صور تشكل جريمة معلوماتية وذلك بالنص عليها في الفصل الثاني من الباب الرابع من القانون سالف الذكر، وذلك ما سوف نوضحه على النحو الآتي:

1.جاءت المادة 127 من القانون 2000-03 لسنة 2000 بفقرتها الأولى، لتجرم فعل الجاني المخول له بتقديم خدمة البريد السريع أو أحد العاملين لديه، الذي يقوم بفتح أو تحويل أو تخريب البريد خاصّةً إذا كانت محتويات ذلك البريد معلوماتً أو قيامه بانتهاك سرية المراسلات، فإذا ما قام الشخص بالأفعال

(1) الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 15-06 المؤرخ في 15 فبراير 2015 يعدل ويتمم القانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية العدد 08، الجزائر، 2015،ص4.

المذكورة سابقاً يعد مرتكباً لأحد صور الجريمة المعلوماتية كون أن محل الجريمة فيها هو المعلومات، أما الفقرة الثانية فإنها تجرّم الانتهاكات الصادرة عن الاشخاص المرخص لهم بتقديم خدمة مواصلات سلكية ولاسلكية أو احد العاملين لديهم والتي تمس بسرية المراسلات سواء كانت صادرة أو مرسلة او مستقبلة من خلال شبكات الاتصال السلكية واللاسلكية، فمثلاً الشخص الذي يقوم بالدخول إلى بيانات ورسائل الأشخاص كونه يقدم خدمة الاتصالات ويستطيع الوصول من خلالها إلى رسائل الأشخاص، وهو ما يجعل منه متابعاً بأحد الجرائم المعلوماتية بصورة انتهاك سرية المراسلات عن طريق استغلاله لتقديمه خدمة الاتصالات سواء كانت سلكية أو لاسلكية[1]، وعاقب عليها المشرع بالحبس من 3 أشهر إلى 5 سنوات والغرامة من30.000 دج إلى 500.000 دج، وذلك طبقا لنص المادة 137 من قانون العقوبات، وفقاً للإحالة الواردة في المادة 127 من القانون 2000-03.

2. الملاحظ على المادة 135 أنها تعاقب على فعل الاستغاثة الكاذبة أو الخادعة التي قد يكون من ورائها مكيدة، ونرى أن المشرع قد حدد الوسيلة التي يتم بها ارتكاب الجريمة ألا وهي اللاسلكي الكهربائي وهو احد التكنولوجيات التي تعتمد على الاشارات الكهرومغناطيسية، ومن هذا المنطلق نرى بأنها تشكل جريمةً معلوماتية كونها تعتمد أساساً لوقوعها على التكنولوجيا[2]، وعاقب عليها المشرع بعقوبة الحبس من شهرين إلى سنة واحدة والغرامة من 10.000 دج إلى 100.000 دج، وهي عقوبة جيدة طالما أن الضرر الناجم عن هذه الجريمة ليس بالضرر الجسيم.

ولم يكتف المشرع الجزائري بذلك في القانون 2000-03 بحيث جرّم عدة أفعال أخرى تدخل في نطاق الجريمة المعلوماتية لا سيما المواد من 127 إلى 149 في الفصل الثاني من الباب الرابع من نفس القانون.

الفرع الثاني: الحماية الجنائية في القوانين المكملة لقانون العقوبات الفلسطيني.

تعددت القوانين الخاصة التي خصّ بها المشرع الفلسطيني نصوصاً متعلقة بالجريمة المعلوماتية كقانون المخدرات، قانون الاتصالات السلكية واللاسلكية، قانون غسل الأموال وتمويل الارهاب، قانون المعاملات الالكترونية، ولعلّ أهم تلك القوانين هو القرار بقانون المتعلق بالجريمة الالكترونية، وهو ما سنبينه على النحو الآتي:

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 2000-03 المؤرخ في 5 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية العدد48، الجزائر، 2000،ص21.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه، ص22.

أولاً: قرار بقانون بشأن مكافحة المخدرات والمؤثرات العقلية.

باستقراء القرار بقانون رقم 18 لسنة 2015 بشأن المخدرات والمؤثرات العقلية، نجد أن المشرع قد نصّ صراحة على ارتكاب الجريمة المعلوماتية وذلك طبقاً للمادة 28 نرى بأن المادة اشتملت على 3 صور للنشاط الإجرامي كالآتي[1]:

أ. إنشاء أو نشر المواقع الالكترونية. جرّم المشرع كل من يقوم بإنشاء المواقع الالكترونية أي يقوم بخلق فضاء الكتروني على شبكة الانترنت وذلك من أجل الترويج أو الاتجار أو التعاطي بالمواد المخدرة، أو يقوم بنشر تلك المواقع لتسهيل حصول الاشخاص على تلك المواد المخدرة سواء من أجل تعاطيها أو المتاجرة بها أو تسويقها، فكلا الفعلين يعدّ جريمة معلوماتية كونها ترتكب في المجال الافتراضي أو المعلوماتي.

ب. تشفير المواقع الالكترونية وحل الشفرات الكترونياً. بحيث يقوم الجاني بعملية التشفير والتي يقصد بها تحويل المعلومات المفهومة إلى معلومات يستحيل على الاشخاص فهمها ويكون الهدف من ذلك الحيلولة دون اكتشاف تلك المواقع ووقوعها بيد السلطات، وكذا قيام الجاني بتجهيز الحاسوب بالتقنيات والبرامج اللازمة لفك الشفرات بحيث يتم تشفير الرسائل بين مروجي أو تجار المخدرات لكي لا يتم فهمها وعند استقبال تلك الرسائل يقوم الحاسوب بفك الشفرات تلقائياً ويرجعها من لغة غير مفهومة إلى لغة مفهومة.

ج. عرض كيفية تصنيع المخدرات والسلائف الكيمائية وكيفية انتاجها وكذا ترويجها وتعاطيها الكترونياً. بحيث يقوم الشخص بوصف عملية تصنيع تلك الممنوعات وذلك بوصف وعرض طرق تحضيرها ومراحل العملية الانتاجية لها كي يتمكن للأشخاص من القيام بعمليات التصنيع للمواد المخدرة، او تمكينهم من اساليب تسويق تلك المواد وطرق تعاطيها، ويكون ذلك من خلال المواقع الالكترونية.

عاقب المشرع الفلسطيني على هذه الجريمة بالأشغال الشاقة لمدة لا تزيد عن 10 سنوات وبغرامة لا تقل عن ألف دينار أردني طبقا لنص المادة 28، وشدد المشرع من العقوبة اذا ما وقعت هذه الجريمة الالكترونية في حالة العود بعد أن كان محكوماً عليه بعقوبة من أجل نفس الجريمة سواء كان ذلك الحكم في بلد أجنبي، وكذا اذا ما قام الجاني بحمل شخص آخر على ارتكاب الجريمة مكرهاً أو بطريق الغش، وتشدد العقوبة أيضاً إذا ما وقعت على قاصر، بحيث ترتفع لتصبح العقوبة الاشغال الشاقة المؤقتة لمدة

[1] دولة فلسطين، القرار بقانون رقم 18 لسنة 2015 بشأن مكافحة المخدرات والمؤثرات العقلية، انظر المادة28.

لا تقل عن عشر سنوات وبغرامة لا تقل عن 3 الاف دينار اردني ولا تزيد عن 15 ألف دينار اردني، وهذا طبقاً لما جاء في نص المادة 29 من القرار بقانون سالف الذكر، فالعقوبة هنا تعتبر رادعة نوعاً ما.

ثانياً: قانون مكافحة غسل الأموال وتمويل الإرهاب.

الملاحظ على المادة الثانية من القرار بقانون رقم 20 لسنة 2015 بشأن مكافحة غسل الأموال وتمويل الإرهاب على ما يلي[1]، لا سيما الفقرة الأولى من المادة الثانية المتعلقة بغسل الأموال أن عملية غسل الأموال قد تتم بالوسائل الإلكترونية وذلك من خلال عمليات التحويل البنكي التي تتم من أجل الإفلات بتلك الأموال من المصادرة ووقوعها بيد السلطات، وأيضاً إذا ما تمت عملية كسر النظام الأمني للمؤسسة المالية بهدف تحويل العائدات الاجرامية المتحصلة من جريمة أصلية من دولة إلى دولة أخرى للحيلولة دون اكتشافها واخفاء طبيعتها الحقيقية، فإذا ما تم ذلك الكترونياً فإنها تعتبر إحدى صور الجريمة المعلوماتية كونها ارتكبت بوسائل إلكترونية.

وبالنسبة لعقوبة جريمة غسل الأموال وردت في المادة 37 من نفس القانون، بحيث يعاقب الجاني بالحبس لمدة لا تقل عن سنة ولا تزيد عن 3 سنوات وغرامة لا تقل عن الأموال محل الجريمة، اما اذا كانت الجريمة الاصلية جناية، يعاقب بالسجن لمدة لا تقل عن 3 سنوات ولا تزيد عن 15 سنة والغرامة لا تقل عن الأموال محل الجريمة، فالملاحظ على العقوبة أنها في صورة الجنحة قد انخفض المشرع بالحد الأدنى للعقوبة مما يؤدي بنا إلى عدم تحقيق العقوبة للغرض منها وهو الردع العام، أما الصورة الثانية فنفس الملاحظة السالفة بالنسبة للحد الأدنى المقررة للعقوبة فهو منخفض نوعاً ما[2].

أما الفقرة الرابعة من المادة الثانية المعلقة بتمويل الإرهاب، الملاحظ أن المشرع الفلسطيني لم يشترط الوسيلة التي يتم بها تمويل الارهاب وطرق جمع الأموال، فقد تتم عملية تمويل الارهاب بطرق الكترونية إذا ما تم إطلاق مواقع الكترونية بهذا الخصوص، أو استخدام مواقع التواصل الاجتماعي من أجل الحصول على دعم مالي للجماعات الارهابية، فالمشرع استخدم مصطلحات مرنة لتشمل جميع الأفعال التي يمكن أن يتم من خلالها ارتكاب الجريمة فهو بذلك فرض الحماية الجنائية من جهة وكافح

---

[1] دولة فلسطين، قرار بقانون رقم 20 لسنة 2015م بشأن مكافحة غسل الأموال وتمويل الإرهاب المؤرخ في 2015/12/30، جريدة الوقائع الفلسطينية عدد ممتاز10، فلسطين، 2015، ص5.

[2] دولة فلسطين، المصدر نفسه ، ص19.

الجريمة المعلوماتية من جهة أخرى من خلال المادة الثانية من القرار بقانون المتعلق بمكافحة غسل الأموال وتمويل الارهاب[1].

عاقب المشرع على هذه الجريمة في المادة 1/43 من نفس القانون سالف الذكر، بالسجن لمدة لا تقل عن 5 سنوات وغرامة لا تقل عن 50.000 دينار، فهذه العقوبة تعتبر عقوبة ردعية وعقوبة صارمة بحق مرتكبها[2].

ثالثاً: قانون الاتصالات السلكية واللاسلكية.

خصص المشرع الفلسطيني للجرائم المرتكبة على وسائل الاتصالات السلكية واللاسلكية أو بواسطتها الفصل الرابع عشر تحت عنوان الجرائم والعقوبات من بالمواد من 86 إلى المادة 100 من القانون رقم 3 لسنة 1960 بشأن الاتصالات السلكية واللاسلكية، وسنتناول بعض هذه الجرائم على سبيل المثال كالآتي:

1. جريمة اعتراض المراسلات.

نص عليها المشرع في المادة 92 من القانون سالف الذكر، بحيث جرّم فعل اعتراض أو إعاقة سير الرسائل والتي يتم تداولها من خلال وسائل الاتصال، ففعل الاعتراض أو الإعاقة يقتضي تدخل الجاني في إيقاف عملية الارسال من أجل معرفة محتوياتها أو تأخير وصولها، وكذا قيام الجاني بتحوير أو شطب محتويات الرسائل، بحيث يقوم الجاني بعد اعتراضه للرسالة بالتعديل عليها بالإضافة أو النقصان أو يقوم بإفراغ الرسالة من محتواها بشكل كامل، فيعتبر بذلك مرتكباً لجريمة اعتراض المراسلات، وعاقب عليها المشرع بالحبس من شهر إلى 6 أشهر إلى سنة واحدة على الأكثر، أو بغرامة لا تقل عن 50 دينار أردني ولا تزيد عن 200 دينار أردني[3]، أو بكلتا العقوبتين، الملاحظ على العقوبة أنها متوسطة الردع.

---

(1) دولة فلسطين، قرار بقانون رقم 20 لسنة 2015م بشأن مكافحة غسل الأموال وتمويل الإرهاب المؤرخ في 2015/12/30، المصدر سابق ، ص5.

(2) دولة فلسطين، المصدر نفسه ، ص21.

(3) دولة فلسطين، قانون رقم3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، جريدة الوقائع الفلسطينية العدد12، فلسطين، 1996، ص37.

2. جريمة اعتراض موجات الغير أو التشويش عليها.

نصت عليها المادة 96 من قانون الاتصالات السلكية واللاسلكية، ومقتضى هذه الجريمة أن يقوم الجاني عمداً بعملية اعتراض الموجات الخاصة بالغير أو بالتشويش عليها، فإن السلوك الاجرامي ينصب على الموجات الكهرومغناطيسية في حال اعتراضها او التشويش عليها وذلك دون ترخيص من وزارة الاتصالات، ومنه يعدم صاحبها فرصة الاستفادة من هذه الموجات واستثمارها في نطاق الاتصالات[1]، وقد عاقب المشرع على هذه الجريمة بالحبس مدة لا تقل عن شهر1 ولا تزيد عن ستة 6 أشهر، أو الغرامة من 50 دينار اردني إلى 200 دينار اردني، أو بكلتا العقوبتين[2]، وذلك وفقاً للسلطة التقديرية لقاضي الموضوع في توقيع العقوبة المناسبة، وهي عقوبة معتدلة في تحقيق الردع لمكافحة هذا النوع من الجرائم، الملاحظ أن المشرع الفلسطيني حاول قدر الإمكان من خلال هذا القانون حصر الجرائم المعلوماتية التي يمكن أن تقع على وسائل الاتصال السلكي واللاسلكي، وذلك للتصدي للجريمة المعلوماتية بكافة صورها.

رابعاً: قانون المعاملات الالكترونية.

جاء هذا القرار بقانون ليواكب التطورات الحاصلة على مستوى التجارة الالكترونية وعمليات التصديق الإلكتروني، فأحاطها بحماية جنائية من خلال القرار بقانون رقم 15 لسنة 2017، والذي جاءَ ليطوّر الخدمات العمومية التي يتم تقديمها الكترونياً، بحيث يحدد هذا القانون الوسائل القانونية التي يتم من خلالها تحسين وتسهيل وتنظيم الخدمات الالكترونية[3]، وبخروج ظاهرة الاجرام المعلوماتي، كان لا بدّ على المشرع حماية تلك الوسائل القانونية التي تعمل على تحسين وتنظيم الخدمة الالكترونية من أي اعتداء عليها لا سيما فيما يتعلق بعملية التوقيع والتصديق الالكتروني، وكذا عمليات تحويل الأموال، ونظراً لأهمية هذه الوسائل أضفى عليها المشرع حمايةً جنائية، وتتجلى أوجه هذه الحماية من خلال تخصيصه للفصل التاسع من نفس القانون للعقوبات التي ترد على الإخلال بأحكام هذا القانون.

عاقب المشرع من خلال المادة 1/44، بإغلاق اي محل أو شركة تقوم بتقديم خدمات المصادقة الالكترونية و/أو التوقيع الالكتروني دون ترخيص، وعاقب في الفقرة الثانية من نفس المادة على إلغاء

---

(1) عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، طبعة 2009، بهجات للطباعة والتجليد، مصر، 2009، ص348.

(2) دولة فلسطين، قانون رقم3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، المصدر سابق، ص38.

(3) نبيل محمود فريد أبو الرب، مفهوم الجرائم المعلوماتية وتحدياتها التشريعية في فلسطين، أطروحة مقدمة استكمالاً للحصول على شهادة الماجستير في القانون العام، جامعة النجاح الوطنية، فلسطين، 2018، ص60.

الرخص أو ايقافها لمددة معينة في حال مخالفة المرخص له شروط الترخيص، وجاءت الفقرة الثالثة من نفس المادة لتعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألفي دينار أردني كل من يقوم بتقديم خدمات المصادقة و/أو التوقيع الالكتروني دون ترخيص.

وعاقبت المادة 45 المرخص له بتقديم الخدمات الالكترونية بالحبس مدة لا تزيد عن 6 أشهر وبغرامة لا تزيد عن الف دينار أردني، في حال تغييره للبيانات المقدمة للحصول على رخصة [1].

ومن هذا المنطلق نرى بأن المشرع الفلسطيني يحاول من خلال هذا القانون فرض حماية جنائية على الأعمال الخدماتية التي تتم بالطرق الالكترونية نظراً لما تقتضيه التطورات الحاصلة في الحياة اليومية.

خامساً: قانون الجرائم الالكترونية.

تبعاً لما يشهده المجتمع الفلسطيني من تزايد في نسب الجريمة المعلوماتية المشرع الفلسطيني من خلال القرار بقانون رقم 16 لسنة 2017 بشان الجرائم الالكترونية لمواجهة هذه الجريمة، ويعتبر هذا القانون الأهم من بين القوانين السابقة، كونه يختص بالجرائم الالكترونية دون غيرها، وسنفصل بهذا القرار بقانون بتقسيم الجرائم إلى جرائم ترتكب بوسائل الكترونية، وأخرى ترتكب عليها.

1- الجرائم التي ترتكب بوسائل الكترونية.

وينقسم هذا النوع من الجرائم إلى 4 أقسام منها ما يرتكب على أمن الدولة، ومنها ما يرتكب ضد الأشخاص ومنها ما يرتكب ضد الأموال ومنها ما يقع على الآداب العامة[2].

أ- الجرائم الواقعة على أمن الدولة.

نصت المادة 1/20 من القرار بقانون سالف الذكر على جريمة إنشاء أو إدارة مواقع الكترونية بقصد نشر أخبار من شأنها تعريض سلامة الدولة أو نظامها العام أو امنها الداخلي أو الخارجي للخطر، فالسلوك الاجرامي لهذه الجريمة يتمثل في إنشاء المواقع الالكترونية على شبكة الانترنت والتي يكون الهدف من ورائها تهديد سلم وأمن الدولة للخطر كنشر الأخبار الكاذبة التي تمس بأمن الدولة، ويعاقب عليها بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أدرني ولا تزيد عن خمسة آلاف دينار

[1] دولة فلسطين، القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الالكترونية المؤرخ في 2017/7/9، جريدة الوقائع الفلسطينية عدد ممتاز14، فلسطين، 2017، ص12، ص13.
[2] نبيل محمود فريد أبو الرب، مرجع سابق، ص61.

أردني، أو بكلتا العقوبتين، وهي عقوبة رادعة تؤدي الغرض منها في المحافظة على أمن الدولة من خطر الجرائم المعلوماتية الهادفة لزعزعة استقرار الأمن[1].

أما الفقرة الثانية من المادة 20 فقد نصت على جريمة ترويج الأخبار التي تمس بأمن الدولة ونظامها العام وأمنها الداخلي أو الخارجي، فالسلوك الاجرامي هنا ينصب على ترويج ونشر المواقع الالكترونية التي تهدف إلى نشر الاخبار التي من شأنها المساس بأمن الدولة، وعاقب عليها المشرع بالحبس مدة لا تزيد عن سنة أو الغرامة التي لا تقل عن مائتي دينار أردني أو بكلتا العقوبتين، وهي عقوبة رادعة كون أن مرتكبها لا ينشأ المواقع ويديرها بل يروّج لها[2].

وجاءت الفقرة الثالثة من المادة 20 لتضاعف العقوبة المقررة في الفقرتين السابقتين أذا ما ارتكبت تلك الأفعال في حالة الطوارئ[3].

ب-الجرائم ضد الأشخاص.

وفي هذا النوع من الجرائم يكون الاشخاص محلاً لارتكاب الجريمة أي ترتكب عليهم، وسنتناول المادة 15 كمثال على هذا النوع من الجرائم، والتي نصت على جريمة التهديد، بحيث جاءت الفقرة الأولى لتعاقب على التهديد أو الابتزاز لحمل المجني عليه على القيام بعمل أو الامتناع عن القيام بعمل حتى ولو كان مشروعاً، وعاقب عليها المشرع بالحبس أو بغرامة لا تقل عن ألفيّ دينار ولا تزيد عن خمسة آلاف دينار، أو بكلتا العقوبتين[4].

وجاءت الفقرة الثانية لتعاقب على الابتزاز أو التهديد بارتكاب جناية أو كان ذلك التهديد مخلاً بالشرف أو الاعتبار، فيعاقب الجاني بالأشغال الشاقة المؤقتة والغرامة من ألفيّ دينار أردني ولا تزيد عن خمسة آلاف دينار أردني[5].

أما بالنسبة للعقوبة فقد اشتملت المادة على عقوبتين الأولى عقوبة جُنَحية والثانية جنائية، وهو الأمر الذي من الممكن ان يؤدي إلى الخروج عن رؤية المشرع التجريمية[6]، وذلك كون أن المشرع ذكر

---

(1) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية المؤرخ في 2017/7/9، جريدة الوقائع الفلسطينية العدد ممتاز14، فلسطين، 2017، ص22، المادة 20، انظر الملحق رقم 2.
(2) دولة فلسطين، المصدر نفسه ،ص22، انظر المادة 20.
(3) دولة فلسطين، المصدر نفسه ، ص22، انظر المادة 20.
(4) دولة فلسطين، المصدر نفسه ، ص21، انظر المادة 15.
(5) دولة فلسطين، المصدر نفسه ، ص21، انظر المادة 15.
(6) نبيل محمود فريد أبو الرب، مرجع سابق، ص64.

مصطلح الاشغال الشاقة المؤقتة ومصطلح الغرامة، مما يوضح لنا تناقض في هذه العقوبات كون أن النظام العقابي لم ينص على الغرامة كعقوبة جنائية وإنما هي عقوبة جنحية، الأمر الذي قد يؤدي بالقضاة إلى النطق بأحكام تخرج عن الإرادة التي يبتغيها المشرع من العقوبة.

ج-الجرائم ضد الأموال.

وهي تلك الجرائم التي ترتكب على الأموال من خلال الوسائل الالكترونية، وسنذكر جريمة منها على سبيل المثال لا الحصر، نصت المادة 18 من القرار بقانون على جريمة غسل الأموال، بحيث يتمثل السلوك الاجرامي المنصوص عليه بها في إنشاء مواقع الكترونية أو تطبيقات أو حسابات الكترونية أو نشر معلومات يكون الهدف منها ارتكاب جريمة غسل الأموال أو تمويل الإرهاب، بحيث أن هذه الجريمة لا تقوم إلا بإثبات الركن المعنوي لها وهو القصد الجنائي، والقصد هنا يتمثل في أن يكون الهدف من وراء تلك المواقع والتطبيقات والحسابات هو ارتكاب جريمة غسل الأموال وتمويل الإرهاب لكي تكون قائمة[1].

عاقب عليها المشرع بالأشغال الشاقة المؤقتة مدة لا تقل عن 10 سنوات، وبغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني[2]، فالملاحظ على هذه العقوبة على الرغم من كونها رادعة وصارمة بحق مرتكبها لتكافح كافة أشكال الاجرام المعلوماتي، إلا أن المشرع قد جمع بين عقوبتين جنائية وجنحية وهو ما يعتبر تناقضاً في النص قد يؤدي إلى عدم تحقيق الهدف من العقوبة الذي يريده المشرع أثناء تطبيق النص من طرف قضاة الموضوع.

د- الجرائم المخلة بالآداب العامة.

وهي الجرائم التي من شأنها أن تمس بالنظام العام وبالآداب العامة كجرائم الابتزاز مثلاً، وقد نصت المادة 16 على عدة صور تشكل اعتداءً على الآداب العامة، بحيث جرّمت في فقرتها الأولى إنتاج كل ما يمس بالآداب العامة أو الاعداد له أو تهييئه بقصد استغلاله أو توزيعه أو عرضه على الغير باستخدام الوسائل الالكترونية أياً كانت، وعاقب عليها المشرع بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، او بكلتا العقوبتين[3].

---

(1) نبيل محمود فريد أبو الرب، مرجع سابق، ص65.

(2) دولة فلسطين القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية المؤرخ في 2017/7/9، المصدر سابق، ص22، انظر المادة 16.

(3) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية المؤرخ في 2017/7/9، المصدر سابق، ص21، انظر المادة 16.

كما نصت الفقرة الثانية من المادة 16 على تجريم فعل إنشاء المواقع أو التطبيقات أو الحسابات الالكترونية ونشر المعلومات على الشبكة الالكترونية، والتي تروّج لما يمس بالآداب العامة، ويعاقب الفاعل بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، او بكلتا العقوبتين.

وجاءت الفقرة الثالثة لتشدد العقوبة إذا ما كان الفعل موجهاً إلى طفل، فتصبح العقوبة الأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني[1].

وفي نفس الصدد جاءت الفقرة الرابعة أيضاً لتشدد العقوبة إذا ما كان المحتوي الذي يمس بالآداب العامة على هيئة طفل أو يحاكي الطفل، فتصبح العقوبة الأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات والغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني[2]، فالعقوبة هنا كانت رادعة بشكل كبير لمرتكب هذا النوع من الجرائم المعلوماتية الماسة بالآداب العامة، إلا أن الملاحظات ذاتها تتكرر بشأن الجميع بين عقوبتين جنائية وجنحية، وكذا عدم تعريف المشرع للآداب العامة وعدم تحديد ما يمكن أن يشمله هذا المصطلح من مفاهيم.

2- الجرائم الماسة بأنظمة المعالجة الآلية.

سنتناول بالشرح والتحليل لجريمة واحدة المثال لا الحصر، فبالرجوع إلى القرار بقانون رقم 16 لسنة 2017 لا سيما المادة 5 منه[3]، بحيث يتمثل النشاط الاجرامي لهذه الجريمة بفعلي الإعاقة أو التعطيل لعملية الدخول للأجهزة أو الوصول للخدمة أو مصادر البيانات، ففعل الإعاقة أو التعطيل قد يكون عن طريق إطلاق برامج تؤدي إلى تعطيل عمل الأجهزة كالقنبلة المعلوماتية، بحيث يتم ذلك من خلال الشبكة الإلكترونية من أجل عدم الوصول لتلك المعلومات والبيانات وعدم تمكين الأشخاص من الدخول للأجهزة، وعاقب المشرع على هذه الجريمة بالحبس أو بالغرامة التي لا تقل عن 200 دينار أردني ولا تزيد على 1000 دينار أردني، وهي عقوبة رادعة بالشكل الذي يعمل على مواجهة الجريمة المعلوماتية المرتكبة بصورة التعطيل أو الإعاقة.

---

[1] دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية المؤرخ في 2017/7/9 ، المصدر سابق، انظر المادة 16.

[2] دولة فلسطين، المصدر نفسه، انظر المادة 16.

[3] دولة فلسطين، المصدر نفسه، انظر المادة 5.

وتعقيباً على العقوبات التي رصدها المشرع الفلسطيني من خلال القرار بقانون بشأن الجرائم الإلكترونية نجد بأن العقوبات كانت قاسية ورادعة إلى حد كبير الأمر الذي يؤدي إلى تحقيق الردع العام والخاص وهو الغرض من وضع العقاب، إلا أنه قد لا يكفل عملية إصلاح وتأهيل المسجونين بقدر إيلامهم.

المطلب الثاني: الحماية الجنائية في النصوص المتعلقة بالملكية الفكرية

سنتعرض في هذا المطلب للحماية الجنائية من خلال النصوص المتعلقة بالملكية الفكرية والتصدي للجريمة المعلوماتية من خلالها، فسنتطرق لقانون الملكية الفكرية الجزائري كفرع أول، وقانون الملكية الفكرية الفلسطيني كفرع ثانٍ.

الفرع الأول: الحماية من خلال نصوص الملكية الفكرية في التشريع الجزائري

سنتناول من خلال هذا الفرع مدى حماية المشرع الجزائري لبرامج الكمبيوتر من خلال نصوص قانون براءات الاختراع وكذا قانون حق المؤلف والحقوق المجاورة له.

أولاً: الحماية الجنائية لبرامج الكمبيوتر من خلال نصوص قانون براءات الاختراع.

قانون براءات الاختراع الصادر بموجب المرسوم التشريعي رقم 93-07 لسنة 1993 وكذا الأمر 03-07 لسنة 2003، سنحاول شرح قابلية البرامج للحماية من خلال نصوص براءات الاختراع[1]، وتعرف براءة الاختراع على أنها شهادة تمنحها الدولة ويتمتع صاحبها بحق احتكار استغلال اختراعه لمدة معينة بمعايير معينة، هي وثيقة تسلم لحماية اختراع، وهذا كما جاء تعريفها بالمادة 1 من الامر 03-07 لسنة 2003، لكي تتحقق براءة الاختراع يجب أن تتوفر عدة شروط والتي تتمثل في الآتي:

- شرط الابتكار.
- أن يكون الاختراع جديد.
- ان يكون الاختراع قابلاً للاستغلال الصناعي[2].
- المشروعية.

(1) خثير مسعود، مرجع سابق، ص68.
(2) عفيفي كامل عفيفي، مرجع سابق، ص 66.

في حال توفر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي من خلالها يتمتع المخترع بحق استغلال اختراعه، والتمتع بالحماية القانونية المقررة لهذا الغرض. ويبقى السؤال مطروحاً هل تستفيد برامج الكمبيوتر من الحماية بواسطة براءات الاختراع؟

التشريعات المعاصرة تستبعد حماية البرامج المعلوماتية من خلال نصوص براءات الاختراع لأحد سببين وهما، تجرد البرامج من أي طابع صناعي، أو صعوبة البحث في كون البرنامج جديداً من أجل تقدير منح استحقاق البرنامج لبراءة الاختراع، بحيث يجب لتقديرها أن يكون هناك للجهة المقررة دراية كبيرة في المجال المطلوب منحه براءة الاختراع فيه، هذا بالإضافة إلى التحفظ العملي الذي يقوم به أصحاب البرامج المعلوماتية، والسبب في ذلك يرجع إلى ادراكهم للصعوبات التي تواجههم من أجل الحصول على براءة الاختراع[1].

ثانياً: الحماية الجنائية لبرامج الكمبيوتر من خلال نصوص حق المؤلف.

نظم المشرع الجزائري قانون الملكية الأدبية والفنية بمقتضى الأمر 73-14 المؤرخ في1973/4/3 المعدل والمتمم بموجب الأمر رقم 03-05 المؤرخ في 2005/7/19 المتعلق بحق المؤلف والحقوق المجاورة.

لم يدرج المشرع الجزائري صراحةً برامج الكمبيوتر ضمن المصنفات الخاضعة لحماية حق المؤلف، وموضوع حق المؤلف هو المصنف الأدبي والفني، كما نصت المادة 2 من الأمر 73-14 على المصنفات التي تشملها الحماية، فنص المادة 2 وإن كان لم ينص صراحة على حماية البرامج المعلوماتية في إطار حق المؤلف، وبالرغم من عدم النص عليها فإن بعض المتخصصين يرون إمكانية حماية البرامج نظراً للصياغة المرنة للمادة عند ذكر المصنفات، بمعنى آخر يمكن إصباغ الحماية على برامج الحاسب الآلي كمصنفات فكرية ضمن عمومية نص المادة 2 في شأن المصنفات التقليدية المحمية[2].

[1] آمال قارة، مرجع سابق، ص136،ص137.
[2] آمال قارة، مرجع نفسه ، ص138.

وبعد تعديل الأمر 73-14 بموجب الأمر 97-10 المعدل والمتمم للأمر رقم 03-05 لمتعلق بحق المؤلف والحقوق المجاورة، نجد أن المشرع قد وسع من قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي ضمن قائمة المصنفات الأصلية الجديرة بالحماية، وفقاً للمادة 4 منه[1].

ونظراً لما تتعرض له برامج الكمبيوتر من اعتداءات فإن أغلب التشريعات لم تخلو من حماية جنائية لكون الحماية المدنية وحدها لا تردع هذه الاعتداءات، فالحماية الجنائية لما تشتمل عليه من عقوبات رادعة وزاجرة تكفل حماية أكثر فعالية لحق المؤلف، حيث نص المشرع الجزائري في المواد 151 إلى 159 من قانون رقم 03-05 على جرائم وعقوبات التي تمس الاعتداء على حق المؤلف[2]، وسنتناول تلك الجرائم على النحو الآتي:

1- جريمة التقليد.

لم يعرفها المشرع الجزائري، واكتفى ببيان الأفعال التي تشكل جريمة التقليد، فكل اعتداء على الحق الأدبي أو المالي لمؤلف البرنامج يشكل فعلاً من أفعال التقليد. نصت المادة 151 من الأمر رقم 03-05 عن قيام جنحة التقليد في الحالات الآتية:

- الكشف غير المشروع للمصنف، فالحق عن الكشف عن المصنف مضمون لصاحب المصنف، وبالتالي فإن عملية الكشف عن البرنامج وإظهارها للعلن من قبل الغير الذي لم يحال له الحق في الكشف عنه يعد اعتداء غير مشروع ويدخل تحت نطاق التجريم.
- المساس بسلامة البرمجية، للمؤلف وحده الحق في تعديل أو تحوير أو تغيير أو حذف أو الإضافة في برنامجه، ولا يحق للغير الاعتراض على ذلك إلا إذا كان فيه إخلالاً أو مساساً بمصالحهم[3].
- استنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة.

ويعتبر هذا السلوك الاجرامي من أخطر واشهر عمليات التقليد والقرصنة المعلوماتية لسهولة القيام بها وقلة تكاليفها وارتفاع مداخيلها، ويقصد بالاستنساخ هو كل عملية الهدف منها الاعتداء على البرامج محل الحماية بأي طريقة، شريطة أن يصحب ذلك السلوك عدم رضا المؤلف، وتجدر الإشارة في جريمة

---

(1) خثير مسعود، مرجع سابق، ص78.

(2) لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند اولحاج-البويرة، الجزائر، السنة الجامعية 2014-2015،ص51،ص52.

(3) خثير مسعود، مرجع سابق، ص89-ص91.

التقليد أنها لا تشترط قصداً جنائياً خاصاً واكتفت بالقصد العام والمتمثل في علم الجاني واتجاه إرادته نحو ارتكاب الجريمة[1].

2- الجرائم الملحقة بجريمة التقليد.

- استيراد أو تصدير برامج مقلدة.

يتضح لنا من خلال هذه الفقرة أن المشرع الجزائري قد بسط حمايته سواء بقانون الدولة الجزائرية أو بقانون دولة اجنبية شرط ان يكون يتمتع بالحماية في دولته، كما يشترط لقيام هذه الجريمة كذلك عدم موافقة المؤلف، وبذلك فهي تشترك مع جرائم التقليد كون ان الموافقة المطلوبة هي موافقة كتابية، وهذا يعني أن الموافقة اللاحقة أو الشفوية أو الضمنية لا تنهي المتابعة[2].

- بيع برامج أو تأجير أو وضع رهن التداول لبرامج مقلدة.

يتمثل النشاط الاجرامي لهذه الجريمة في حال التعامل مع برامج مقلدة سواء بالبيع أو الإيجار أو التداول، ويكون البرنامج مقلداً إذا كان مشابها للبرنامج المحمي قانوناً، والعبرة تكون بأوجه الشبه لا الاختلاف لما لها من تأثير في التعامل.

والبيع يقصد به نقل حق استغلال البرنامج إلى الغير مقابل ثمن معين، سواء كان هذا البيع ينطوي على النشر أو الاستعمال أو الترجمة للبرنامج المقلد، أما الإيجار فهو وضع البرنامج المقلد أو نسخ منه لدى المستأجر قصد تمكينه من استعمالها لمدة زمنية معينة مقابل مبلغ مالي معين، والتداول يقصد به وضع البرنامج بين يدي الغير لاستعمالها بمقابل أو دون مقابل، أو الانتفاع بها لمدة زمنية محدودة أو غير محدودة[3].

- المشاركة في تقليد برنامج.

وتعتبر هذه الصورة من جرائم التقليد كون أن الشريك تطبق عليه القواعد العامة للمساهمة الجنائية.

- رفض دفع المكافأة المستحقة عمداً لمؤلف البرنامج.

---

(1) خالد مصطفى فهمي، الحماية القانونية لبرامج الكمبيوتر، بدون رقم طبعة، دار الجامعة الجديدة للنشر، مصر، 2005،ص119.

(2) خثير مسعود، مرجع سابق، ص97.

(3) خثير مسعود، مرجع نفسه، ص98.

تقوم هذه الجريمة في حال امتناع الشخص المكلف بدفع المكافأة المستحقة لمؤلف البرنامج عمداً، وتكون هذه المكافأة جرّاء تنازل المؤلف عن حق من حقوقه المادية سواء كلها أو جزء منها، وهذا طبقا للمادة 95 من الأمر 03-05[1].

يعاقب مرتكب هذه الجرائم بالحبس من 6 أشهر إلى 3 سنوات والغرامة من 500.000 دج إلى 1.000.000 دج وهذا طبقا لنص المادة153 من قانون حق المؤلف والحقوق المجاورة له، وتضاعف العقوبة في حالة العود استناداً للمادة 156[2].

الفرع الثاني: الحماية الجنائية من خلال نصوص الملكية الفكرية في التشريع الفلسطيني.

سنتناول في هذا الفرع مدى حماية التشريعات السارية في فلسطين بخصوص الملكية الفكرية سواء من خلال قانون امتيازات الاختراعات والرسوم وهو القانون رقم 22 لسنة 1953، وكذا الحماية من خلال نصوص قانون حقوق الطبع والتأليف وهو القانون رقم 46 لسنة 1911 الصادر عن الانتداب البريطاني وتطبيقه على فلسطين سنة 1924.

أولاً: الحماية الجنائية لبرامج الكمبيوتر من خلال قانون امتيازات الاختراع والرسوم.

صدر هذا القانون سنة 1953، وقد اشتمل على الاحكام المتعلقة بالاختراع وشروطه وكيفيات تسجيل براءة الاختراع والحصول عليها، والحقوق المترتبة عنها للمخترع، وباستقراء نصوص القانون سابق الذكر نجد أن موقفه من حيث حماية برامج الكمبيوتر من خلال نصوص براءات الاختراع قد سايرت موقف المشرع الجزائري من حيث إصباغ الحماية على تلك البرامج من خلال نصوص براءات الاختراع، فكلا القانونين لم يعترف بالحماية لبرامج الكمبيوتر من خلالها، ولعل السبب في ذلك يعود إلى صعوبة توفر الشروط المتعلقة بمنح براءة الاختراع عند إسقاطها على برامج الكمبيوتر.

ذهب جانب من الفقه إلى اعتبار البرامج من قبيل المبتكرات التي يتمتع صاحبها بحث ملكية الاختراع، وبالتالي إذا ما توافرت شروط منح براءة الاختراع ألا وهي شرط الابتكار، ان يكون جديداً، ان يكون الاختراع قابل للاستغلال الصناعي وأن يكون مشروعاً، فبمجرد تحقق هذه الشروط فإن العقود الواردة عليه – الاختراع– وبوصفه محلاً لحق استئثاري تسمح بنقل السلطات التي يخولها لصاحبه كلها أو

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة له المؤرخ في 2003/7/19 المعدل والمتمم للأمر رقم 14/73، الجريدة الرسمية ، الجزائر، 2003، المادة 95.
(2) الجمهورية الجزائرية الديمقراطية الشعبية، المصدر نفسه ، المادة 153.

بعضها من خلال عقد البيع أو عقود الترخيص بالاستعمال – عارية الاستعمال–، وعليه فنطبق الأحكام المتعلقة بعقد البيع في القانون المدني بالإضافة إلى تطبيق الأحكام الخاصة بالتنازل عن براءات الاختراع[1].

ويرى القائلون بالحماية لقوانين براءة الاختراع ان برامج الكمبيوتر ولأنها تستعمل للتعامل مع آلات الحاسوب وإدارتها فهي بذلك تصبح جزء منها، ولمّا كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب، فهي بذلك تصبح قابلة للبراءة.

غير أنه من الصعب توفير حماية ناجعة للمعطيات بالرجوع إلى قانون الملكية الصناعية ويتعلق الأمر أساساً بتوافر شرطين هما[2]:

– شرط الجدّة: ويقصد به عدم علم الغير بسر هذا الابتكار أو الاختراع قبل طلب البراءة، ويتضح من ذلك أنه يجب أن يكون الابتكار أو الاختراع سراً لا يتسرب إلى علم الغير قبل أن يتقدم الطالب بطلب براءة الاختراع، وبمفهوم المخالفة يعني أن عدم انطباق هذا الوصف جدة الاختراع في حالة تفشي هذا السر إلى علم الغير قبل تقديم طلب البراءة[3]، فهذا الشرط بحد ذاته يصعب التحقق من كون طالب البراءة قد تم إفشاء سر اخترعه أم لا، فهو يحتاج إلى جهود كبيرة للتحقق من مدى جدّة الاختراع.

– القابلية للاستغلال الصناعي: يقصد بها قابلية الاختراع للاستخدام، دون ان يتحقق ذلك بالفعل، إذ يتوقف ذلك على الفرص السانحة، فقابلية الاختراع للاستخدام الصناعي والتطبيق العلمي فيها هي التي تعطي الاختراع الصفة الصناعية سواء كانت هناك فرصة أم لا، ويقصد بالصناعة في هذا المجال جميع ضروب النشاط الصناعي ونظم الصناعات الزراعية والاستخراجية[4].

وفي سياق متصل هناك من يضيف على تلك الصعوبات أن عقد الترخيص في مجال براءات الاختراع يفرض التزاماً باستغلال البراءة محل الترخيص بينما هذا الشيء غير مقبول ومستبعد في مجال البرامج الالكترونية من خلال عقد الترخيص باستعمالها، ويرى جانب من الفقه أن الابتكار يجب أن ينصّب على أشياء ملموسة حتى تتم حمايته من خلال النظام القانوني لبراءات الاختراع، فالابتكار يجب

(1) محمد موسى خلف، حماية برامج الحاسب الآلي بين براءة الاختراع وحق المؤلف، مجلة الفكر، العدد الثالث عشر، جامعة محمد خيضر بسكرة، 20، ص60.

(2) بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، الجزائر، 2013، ص4.

(3) عفيفي كامل عفيفي، مرجع سابق، ص67.

(4) خثير مسعود، مرجع سابق، ص70.

أن يكون مقروناً بالابتكار الصناعي، كأن يكون انتاج صناعي جديد او طريقة صناعية جديدة أو حتى تطبيق جديد لوسائل أو طرق صناعية معروفة، وبالتالي لا يمكن اعتبار برامج الكمبيوتر من قبيل الأشياء المادية الملموسة التي تجسدت في ابتكار اقترن بالصناعة، وقانون امتيازات الاختراع المطبق في الضفة الغربية رقم 22 لسنة 1953 لم يذكر كلمة ابتكار بل ذكر كلمة اختراع في المادة الثانية منه وتعرف كلمة اختراع بأنها" **نتاجاً جديداً أو استعمال أية وسيلة اكتشفت أو عرفت او استعملت بطريقة جديدة لأية غاية تجارية.**" وهو ما يؤكد قصور الحماية على برامج الكمبيوتر من خلال نصوص قانون امتيازات الاختراع والرسوم[1].

ثانياً: الحماية الجنائية لبرامج الكمبيوتر من خلال قانون حقوق الطبع والتأليف.

وهو القانون رقم 46 لسنة 1911 الصادر عن الانتداب البريطاني وتطبيقه على فلسطين سنة 1924، يتضح لنا أن قانون حقوق الطبع والتأليف قد أضفى الحماية على برامج الكمبيوتر، وذلك باعتبارها أحد المصنفات الأدبية أو الفنية وهذا ما نصت عليه المادة الأولى من القانون سالف الذكر، نظراً لعمومية النص، ومن هذا المنطلق نرى بأن المشرع قد خصها بحماية جنائية لدرء أي اعتداء قد يقع على تلك المصنفات المحمية بموجب قانون حقوق الطبع والتأليف لسنة 1911، وبعد تعديل هذا القانون سنة 1924 وجعله ساري المفعول في فلسطين كونها منتدبة من بريطانيا، جاءت المادة الثالثة من هذا القانون لتبين لنا الافعال التي جرّمها لحماية أي مصنف سواء كان أدبيا أو فنياً أو موسيقياً أو تمثيلياً.

وكون أنه ينتج عن ذلك المصنف حقوقاً أدبية والتي تعرف بأنها الدرع الواقي الذي بمساعدته يثبت المؤلف شخصيته بمواجهة معاصريه ومواجهة الاجيال الماضية والقادمة، وكذا ينتج حقوقاً مالية، وبمقتضى هذا الحق يكون للمؤلف حق استثمار مصنفه والحصول من وراء نشره او إذاعته أو ترويجه أو نسخه أو السماح باستعماله على مداخيل مادية "مالية" وهذه الحقوق تخضع لجميع التصرفات القانونية وتشمل حق النشر وغيره من الحقوق[2]، لذلك وجب أن تكون هناك حماية جنائية من أي اعتداء بأنها وقد ذكرت المادة العديد من الاعتداءات على النحو الآتي:

---

(1) محمد موسى خلف، مرجع سابق، ص61.

(2) حقاص صونية، حماية الملكية الفكرية الأدبية والفنية في البيئة الرقمية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماجستير تخصص المعلومات الالكترونية، الافتراضية واستراتيجية البحث عن المعلومات، جامعة منتوري قسنطينة، الجزائر، 2012، ص32-ص36.

- بيع أو تأجير نسخ مقلدة من مؤلف لا تزال حقوق طبعه محفوظة.
- بيع أو تأجير نسخ مقلدة من مؤلف أو عرضها أو قدمها للبيع أو الأجرة بقصد التجارة.
- توزيع نسخ مقلدة بقصد التجارة أو بقصد الاضرار بحقوق صاحب الطبع والتأليف.
- العرض العلني بقصد التجارة نسخاً مقلدة من مؤلف.
- استورد إلى فلسطين نسخاً مقلدة من مؤلف للبيع أو الأجرة.

بالنظر إلى تلك الاعتداءات نجدها ناتجة عن جريمة تقليد، بحيث تتم عملية التقليد ثم بعد ذلك تتم عملية البيع أو الايجار لأي غرض كان، وهو ما يجعلنا نقسم هذه الجرائم إلى قسمين كالآتي:

1. جريمة التقليد.

هذه الجريمة لم ينص عليها قانون حقوق الطبع والتأليف واكتفى بالجرائم الملحقة بجريمة التقليد، بحيث أن جريمة التقليد– كما سبق أن رأينا عند تناول الحماية الجنائية من خلال نصوص حقوق المؤلف الجزائري– يقوم ركنها المادي على 3 صور وهي كالآتي:

– الكشف غير المشروع عن البرمجية: بحيث أن لمؤلف المصنف وحده حق الكشف عن مؤلفه، سواء كان ذلك باسمه أو باسم شخص آخر، فإن عملية الكشف عن البرمجية من طرف شخص آخر يعتبر اعتداء غير مشروع على أحد حقوق المؤلف ويعتبر بذلك مرتكباً لأحد سلوكيات جريمة التقليد.

– المساس بسلامة البرمجية: وينطوي ذلك على حق المؤلف وحده في تعديل أو تحوير او اضافة أو حذف أو تغيير أي شيء في برنامجه، فإذا ما تم ذلك الفعل من طرف أي شخص آخر لم يخول له المؤلف ذلك الحق يعتبر مرتكباً لجريمة التقليد من خلال فعل المساس بسلامة البرمجية.

– استنساخ البرنامج بأي أسلوب من الأساليب في شكل نسخ مقلدة[1]: وهي قيام الغير بأي فعل من شأنه الاعتداء على البرنامج محل الحماية، سواء عن طريق نسخه أو أي فعل آخر.

2. الجرائم الملحقة بجريمة التقليد.

وهي تلك الجرائم التي تقع بعد أن يتم تقليد البرنامج بأي صورة من الصور سالفة الذكر، وقد نص عليها قانون حقوق الطبع والتأليف لسنة في 1924 في المادة الثالثة منه، وسنفصل فيها على النحو الآتي:

[1] خثير مسعود، مرجع سابق، ص 92.

أ. جريمة استغلال البرامج المقلدة.

قد يكون استغلال البرامج المقلدة بقصد التجارة وقد يكون بدافع شخصي وقد يكون بهدف الاضرار بحقوق صاحب الطبع والتأليف، وقد حدد صور هذا الاستغلال في 4 صور وهي كالآتي:

– البيع: وهو الذي بمقتضاه يتم نقل حق استغلال البرنامج إلى المشتري مقابل ثمن معين وسواء كان الاستغلال ينطوي على نشر أم استعمال أم ترجمة للبرنامج المقلد.

– العرض للبيع: لم يكتف المشرع بالعقاب على البيع فقط، بل تعدى ذلك ليجرّم عرض بيع البرامج المقلدة، فهو لا ينتظر إلى حين ان يتم البيع بل ان مجرد عرض بيع تلك البرامج المقلدة يعتبر جريمة.

– الإيجار: ويقصد به قيام شخص ما بتأجير تلك البرامج المقلدة للمستأجر مقابل مبلغ مالي معين، على أن يتمكن من استغلاله لفترة محددة[1].

– التوزيع: وتقتضي هذه الصورة أن يقوم الشخص بحيازة برامج مقلدة يعمل على توزيعها سواء كان ذلك لقاء الحصول على مبالغ مالية أو أدبية أو كان ذلك دون مقابل، وينطوي على هذا التصرف نقل الملكية او الاستغلال أو التصرف أو الاستعمال.

ب.جريمة استيراد برامج مقلدة قصد بيعها او تأجيرها.

ويستشف من ذلك أن الحماية تطال المصنفات الأجنبية عند إدخالها لفلسطين قصد بيعها او تأجيره، فيشترط لهذه الجريمة عدم موافقة المؤلف، بحيث لا يعتد بالموافقة الضمنية أو الشفوية بل يجب أن تكون تلك الموافقة كتابية[2]، ويقوم النشاط الإجرامي لهذه الجريمة بإدخال برامج الكمبيوتر إلى الدولة دون موافقة مؤلفها، مع توفر القصد الجنائي لدى مرتكبها[3].

وقد نص قانون حقوق الطبع والتأليف لسنة 1924 في المادة الثالثة منه على عقوبة الغرامة المقدرة ب 250 ملاً عن كل نسخة جرى التصرف فيها على أن لا تتجاوز 50 جنيهاً في المعاملة الواحدة، وفي حال ما إذا ارتكبت في حالة العود فيعاقب المجرم بنفس الغرامة أو بالحبس لمدة شهرين[4].

وفي الأخير نرى بأن نصوص قانون امتيازات الاختراع والرسوم تحتوي على العديد من الصعوبات والتي تحول دون حماية برامج الكمبيوتر من خلال تلك النصوص، بينما نصوص قانون حقوق

---

(1) عفيفي كامل عفيفي، مرجع سابق، ص95،ص96.
(2) خثير مسعود، مرجع سابق، ص97.
(3) عفيفي كامل عفيفي، مرجع سابق، ص92.
(4) دولة فلسطين، قانون حقوق الطبع والتأليف لسنة 1924، أنظر المادة 3 منه.

الطبع والتأليف وكونها جاءت بصياغة عامة فإنه يمكن من خلالها حماية برامج الكمبيوتر باعتبارها مصنفاتً أدبية أو فنية، إلا أن العقوبة التي جاء بها هذا القانون تعتبر عقوبة لا تجدي نفعاً ولا غير رادعة خاصةً إذا ما وقعت تلك الاعتداءات على البرامج التي تشكل قيمة اقتصادية عالية ووقوع الاعتداء عليها قد يحدث ضرراً كبيراً بالمؤلف.

خلاصة الفصل:

اتجه كلا المشرعين الجزائري والفلسطيني قبل وجود نص تجريمي للجريمة المعلوماتية، إلى تطويع نصوص جرائم الأموال المتعلقة بجريمة السرقة، النصب، خيانة الأمانة، فإن المعلوماتية تصلح لأن تكون محلاً لجرائم الأموال خاصة في قانون العقوبات الجزائري وكذا قانون العقوبات المطبق في الضفة الغربية إلا أن محل جريمة خيانة الأمانة وفقاً لما جاء في قانون العقوبات المطبق في قطاع غزة لا يسمح للمعلوماتية أن تكون محلاً للجريمة.

أما من حيث خضوع المعلوماتية للنشاط الإجرامي لجرائم الأموال، فخضوع المعلوماتية لفعل الإختلاس في جريمة السرقة ثار حوله جدلاً فقهيا، ولم يحدد كلا القانونين الجزائري والفلسطيني موقفاً واضحاً من تلك الآراء الفقهية، فالحل الوحيد كان تعديل قانون العقوبات والنص على سرقة المعلومات من كلا المشرعين، أما من حيث خضوعها للنشاط الإجرامي لجريمة النصب فإنه يمكن وقوع فعل الاحتيال على المعلوماتية من طرف المشرع الجزائري إذا كانت تلك المعلومات مادية، ونفس الأمر بالنسبة للقانون الفلسطيني فقد أتاح خضوع المعلوماتية للنشاط الإجرامي لجريمة النصب، وفي جريمة خيانة الأمانة يمكن خضوع المعلوماتية للنشاط الاجرامي وفقاً لما جاء في قانون العقوبات الجزائري ونظيره في الضفة الغربية، ونجد عكس ذلك في قانون العقوبات المطبق في غزة.

بعد تعديل قانون العقوبات الجزائري سنة 2004 جاء بنصوص خاصة بالجريمة المعلوماتية لتجرّم الاعتداءات التي تقع على انظمة المعلوماتية، وجاء بجرائم عدة كجريمة الدخول أو البقاء في نظام المعالجة الآلية للمعطيات، على العكس من ذلك في التشريع العقابي الفلسطيني، بحيث خلا كلا القانونين سواء في الضفة الغربية أو قطاع غزة من نصوص خاصة تجرم الأفعال المرتكبة على المعلوماتية.

جاءت القوانين الخاصة المكلمة لقانون العقوبات في كلا التشريعين الجزائري والفلسطيني بأفعال تعتبر من قبيل الجريمة المعلوماتية إذا ما ارتكبت بالوسائل الالكترونية كقانون غسل الأموال وتمويل الإرهاب، ومن جهة اخرى فإن القوانين الخاصة المتعلقة بالملكية الفكرية حاولت حماية برامج الكمبيوتر من أي اعتداء كقانون حق المؤلف والحقوق المجاورة له وقانون حقوق الطبع والتأليف، على الرغم من ذلك لا يمكن حماية برامج الكمبيوتر من خلال نصوص قوانين براءات الإختراع لصعوبة توافر شروط منح براءة الاختراع في تلك البرامج.

الفصل الثاني

الإطار الإجرائي للجريمة المعلوماتية

تمهيد:

يقتضي مبدأ الشرعية الجنائية أن يكون هناك نص قانوني يجرّم الفعل حتى تكون الجريمة لها وجود قانوني، ويستوي الأمر بالنسبة للشرعية الإجرائية، بحيث بعدد وقوع لجريمة تتحرك عجلة الاجراءات الجزائية لملاحقة مرتكبي الجريمة والكشف عنهم وذلك من أجل تقديمهم للعدالة وتوقيع العقاب عليهم، لكي يقوم جهاز الضبطية القضائية بجمع الاستدلالات، والنيابة العامة تقوم بعملها في استكمال التحقيق الأولي، ويقوم قضاة التحقيق كذلك بأعمال فيما يتعلق بالتحقيق الابتدائي، إلى حين وصول المتهم إلى قضاة الحكم، يجب أن تكون هناك ضوابط قانونية تبين سبل اتخاذ تلك الاجراءات، وتلك الضوابط يحددها قانون الاجراءات الجزائية أو من خلال القوانين الخاصة التي تأتي بنظام إجرائي خاص بجرائم معينة.

فإجراءات المتابعة تمر بعدة مراحل قبل وصول المتهم إلى قضاة الموضوع، وكذا اختصاصات كل جهاز في الوصول إلى الحقيقة، وتلك الاجراءات تتخذ بهدف التوصل إلى الأدلة التي من شانها إثبات ارتكاب الجريمة من طرف الشخص المشتبه به أو ارتكابها من طرف آخر.

والجريمة المعلوماتية وما تمليه من صعوبة في اكتشافها، لا سيما وأنها جريمة ترتكب في العالم الافتراضي في الغالب، وكونها ترتكب بوسائل إلكترونية فإن عملية طمس الادلة لا يستغرق سوى نقرة زر ، لذلك جاء المشرع الجزائري بإجراءات خاصة بهذه الجريمة في القانون رقم 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إلى جانب القواعد العامة المنصوص عليها في الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المعدّل والمتمم المتضمن قانون الاجراءات الجزائية، وذات الأمر بالنسبة للمشرع الفلسطيني فقد جاءت أحكام خاصة تتعلق بإجراءات المتابعة والتحقيق في القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية والعمل إلى جانب ذلك بالقواعد العامة المذكورة في القانون رقم 3 لسنة 2001 المتضمن قانون الاجراءات الجزائية.

وسنقسم الدراسة في هذا الفصل إلى، **المبحث الأول** المكافحة الإجرائية للجريمة المعلوماتية في ظل قانون الاجراءات الجزائية، المطلب الأول قواعد الاختصاص القضائي، المطلب الثاني أعمال التحقيق، **المبحث الثاني** المكافحة الاجرائية للجريمة المعلوماتية في القوانين الخاصة، المطلب الأول أعمال التحقيق الخاصة، المطلب الثاني إنشاء هيئات متخصصة.

المبحث الأول

المكافحة الإجرائية للجريمة المعلوماتية في ظل قانون الاجراءات الجزائية

سنتناول في هذا المبحث أساليب التحري والتحقيق في الجريمة المعلوماتية من خلال ما جاء في قانون الاجراءات الجزائية لكلا المشرعين الجزائري والفلسطيني، وسنقسم الدراسة إلى مطلبين، المطلب الأول: قواعد الاختصاص القضائي، المطلب الثاني: أعمال التحقيق.

المطلب الأول: قواعد الاختصاص القضائي

ونقصد بقواعد الاختصاص القضائي هو النطاق الجغرافي المخول للضبطية القضائية (مأموري الضبط القضائي) والنيابة العامة وقضاة التحقيق والمحاكم لممارسة الصلاحيات المنوطة بهم المنصوص عليها في قانون الإجراءات الجزائية.

الفرع الأول: اختصاص المحاكم

أولاً: الاختصاص النوعي

باستقراء النصوص المتعلقة بالجريمة المعلوماتية في التشريع الجزائري نجد بأن المشرع قد حدد وصفها القانوني فجعل كل الجرائم المعلوماتية ذات وصف جنحة، ومن ذلك فإن المحكمة المختصة نوعياً هي محكمة الجنح، تبعاً للوصف القانوني الذي يلحق بالجرائم المعلوماتية في التشريع الجزائري[1].

كما يؤول الاختصاص في الجريمة المعلوماتية في قانون الاجراءات الجزائية رقم 3 لسنة 2001 الفلسطيني، إذا كانت تحمل وصف جنحة فينعقد الاختصاص لمحكمة الصلح، أما إذا كانت جناية فإن الاختصاص ينعقد لمحكمة البداية، طبقاً لنصوص المواد 166، 167[2].

ثانياً: الاختصاص المحلي

لقد حدد المشرع الجزائري اختصاص المحاكم طبقاً للمادتين 37 و 40 من قانون الاجراءات الجزائية، يتحدد الاختصاص بمكان وقوع الجريمة، محل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو المكان الذي تم في دائرته القاء القبض على أحد هؤلاء الأشخاص.

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم، الجريدة الرسمية العدد 48، الجزائر، 1966، المادة 328.

(2) دولة فلسطين، قانون الاجراءات الجزائية رقم 3 لسنة 2001، المواد 166، 167.

أما الأحداث طبقاً للمادة 32من القانون رقم 15-12 المؤرخ في 15 يوليو 2015 المتعلق بحماية الطفل، فإن المحكمة المختصة هي التي يكون بها محل اقامة الطفل أو ممثله الشرعي، أو المكان الذي وجد به الطفل[1].

وفيما يخص تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى وذلك طبقاً لنص المادة 329 من قانون الإجراءات الجزائية، وذلك في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وغيرها من الجرائم محددة على سبيل الحصر[2].

أما المشرع الفلسطيني فقد حدد الاختصاص الاقليمي للمحاكم بناءً على المكان الذي وقعت فيه الجريمة، أو تختص محكمة محل اقامة المتهم، أو يعود الاختصاص لمحكمة مكان القاء القبض عليه[3].

إلا أنه بخصوص تمديد الاختصاص فإن المشرع الفلسطيني لم ينص على حالات تمديد الاختصاص، فيبقى الاختصاص حسب ما هو محدد في المادة 163 من قانون الاجراءات الجزائية الفلسطيني، إلا أنه استثناءً يجوز للنائب العام أن يطلب من المحكمة المختصة بإحالة ملف الدعوى لمحكمة أخرى من نفس الدرجة إذا رأى أن المحكمة المختصة اقليمياً عند فصلها بالدعوى من شأنه الاخلال بالنظام العام وذلك استناداً للمادة 182 من قانون الاجراءات الجزائية الفلسطيني.

الفرع الثاني: اختصاص الضبطية القضائية.

يمارس أفراد الضبطية القضائية او مأموري الضبط القضائي مهام البحث والتحري عن الجرائم والقيام بجمع الادلة التي تدين المتهم بارتكابه جريمةٍ ما، بحيث يقوم ضباط وأعوان الشرطة القضائية بجمع الاستدلالات من خلال عمليات التفتيش وكذا معاينة مسرح الجريمة ، ومن خلال الصلاحيات الممنوحة لهم في حالة التلبس وسماع الضحية والشهود واحتجاز المشتبه فيهم في حالة وجود دلائل قوية لارتكابهم الجريمة، والقيام بعملية التسرب واعتراض المراسلات وغيرها من الصلاحيات التي تدخل في اختصاصهم النوعي.

---

(1) صديق حياة، خصوصية الجريمة المعلوماتية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2008، ص56، ص57.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المعدل والمتمم، مصدر سابق، المادة 329.

(3) دولة فلسطين، مصدر سابق، المادة 163.

يقصد بالاختصاص المحلي الدائرة الجغرافية التي تمارس فيها الشرطة القضائية الصلاحيات المخولة لها قانوناً، وهو ما جاء في المادة 16 من قانون الاجراءات الجزائية الجزائري بنصها: " **يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة**"[1].

حيث يمارس أفراد الشرطة القضائية اختصاصهم في حدود دائرة عملها بصرف النظر عن مكان وقوع الجريمة، فهي تختص بالبحث والتحري عن الجريمة إذا ما وقعت في دائرة اختصاصها المكاني، أو سواء ألقي القبض على المشتبه فيه في دائرتها أو أن أحد المشتبه فيهم يقيم في دائرتها[2].

إلا أنه يمكن تمديد اختصاصهم في حالة الاستعجال ليشمل كافة دائرة اختصاص المجلس القضائي وقد يمتد ليشمل كافة التراب الوطني، ويكون ذلك بناءً على طلب من قاضي التحقيق المختص قانوناً، على أن يقوم أفراد الضبطية القضائية بإخبار وكيل الجمهورية الذين يباشرون مهمتهم في دائرة اختصاصه بذلك، ويتمتع بعض أصناف الضبطية القضائية باختصاص وطني وهم مصالح الأمن العسكري في الجرائم الماسة بأمن الدولة[3].

ويمتد الاختصاص الاقليمي للضبطية القضائية في جرائم محددة على سبيل الحصر في المادة 7/16 من قانون الاجراءات الجزائية الجزائري وهي جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، إلا أن عملهم يتم في ذلك تحت إشراف النائب العام مباشرةً مع علم وكيل الجمهورية المختص إقليمياً بذلك في جميع الحالات[4].

ذلك يتضح لنا أن المشرع الجزائري أعطى أهمية بالغة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بحيث سمح بتمديد الاختصاص المحلي للضبطية القضائية عند القيام بمهام البحث والتحري، مما يبين لنا خطورة هذا النوع من الجرائم.

أما المشرع الفلسطيني فقد حدد الاختصاص المحلي لمأموري الضبط القضائي لممارسة صلاحياتهم في جمع الاستدلالات والبحث والتحري عن الجرائم بدائرة اختصاص النائب العام الذين

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، مصدر سابق، المادة 16.
(2) عبد الرحمان خلفي، الاجراءات الجزائية في التشريع الجزائري والمقارن، الطبعة الثالثة، دار بلقيس، الجزائر، 2017، ص98،ص99.
(3) عبد الرحمان خلفي، مرجع نفسه، ص99.
(4) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966، مصدر سابق، المادة16.

يمارسون صلاحياتهم تحت إشرافه وذلك طبقاً لما جاء في المادة 19 من قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001.

أما فيما يخص مسألة تمديد الاختصاص المحلي لمأموري الضبط القضائي فإن المشرع الفلسطيني لم ينص في قانون الاجراءات الجزائية على إمكانية تمديد الاختصاص المحلي للضبطية القضائية، مما يفهم منه أن مأموري الضبط القضائي ملزمون بدائرة اختصاص النائب العام الذين يمارسون صلاحياتهم تحت إشرافه.

الفرع الثالث: اختصاص النيابة العامة.

تختص النيابة العامة بتحريك الدعوى العمومية وذلك وفقاً لسلطة الملائمة التي تتمتع بها من أجل تحريك الدعوى العمومية من عدمه، وتقوم بالإشراف على الضبطية القضائية من حيث أعمالها ومشروعيتها، وكذا تقوم النيابة العامة بسماع الضحايا والشهود، والانتقال لمعاينة مسرح الجريمة بوجود قاضي التحقيق، ويكون من اختصاص النيابة العامة منح الإذن المكتوب الموجه للضبطية القضائية من اجل القيام بعملية التفتيش، وكذا منح الإذن للقيام بعملية التسرب في الجرائم المحددة قانوناً والتي تشمل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وكذا تمديد التوقيف للنظر، وغيرها من الصلاحيات المخولة للنيابة العامة في إطار مكافحة الجرائم المعلوماتية والجرائم التقليدية.

يعد وكيل الجمهورية ممثل النيابة العامة على مستوى المحكمة، بحيث يكون مختصاً إقليمياً بإحدى الحالات الثلاث، بمكان وقوع الجريمة أو بمحل إقامة المشتبه فيهم، أو المكان الذي تم إلقاء القبض فيه على أحد المشتبه فيهم، وهذا بالاستناد لنص المادة 37 من قانون الاجراءات الجزائية الجزائري، وهذا يدل على أن وكيل الجمهورية يختص بتحريك الدعوى العمومية في الجرائم الواقعة بتلك الأمكنة التي يتحدد من خلالها اختصاصه المحلي[1].

حيث أنه بموجب المادة 37 من قانون الاجراءات الجزائية الجزائري تم توسيع اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصاً لها من قبل، حيث نصت المادة 37 على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم وذلك في جرائم محددة ألا

[1] عبد الرحمان خلفي، مرجع سابق، ص200.

وهي جرائم المخدرات، الجريمة المنظمة، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف[1].

ومما سبق نرى بأن المشرع الجزائري قد منح للنيابة العامة سلطات واسعة في مجال مكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويتجلى ذلك من خلال منح النيابة العامة سلطات أوسع من حيث اختصاصها المحلي ، وفي إطار مكافحة الجرائم المعلوماتية أصبح بإمكان وكيل الجمهورية تمديد اختصاصه ليشمل دائرة اختصاص المجلس القضائي.

أما المشرع الفلسطيني نستشف الاختصاص المحلي للنيابة العامة من خلال الاختصاص المكاني للمحاكم، فيكون وكيل النيابة مختصاً إقليماً، إذا ارتكبت الجريمة بالمكان الخاضع لدائرة اختصاص المحكمة، أو المحل الذي يقيم فيه المتهم، أو مكان إلقاء القبض عليه، ويمكن للنائب العام ان يقوم بندب وكيل نيابة في دائرة اختصاص محكمة أخرى.

وتجدر الإشارة إلى أنه تم إنشاء نيابة خاصة لمكافحة الجريمة المعلوماتية في فلسطين بموجب قرار صادر عن النائب العام وتتكون هذه النيابة من 26 عضواً مختصين في البحث والتحري عن جرائم التقنية العالية للمعلومات، وتتشكل هذه النيابة الخاصة في كل محافظة من محافظات الوطن، ويتم الإشراف على أعمالها من قبل النائب العام بشكل مباشر[2].

الفرع الرابع: اختصاص قاضي التحقيق.

يمارس قاضي التحقيق صلاحياته بإجراء التحقيق الابتدائي بعد طلب النيابة العامة منه، ويكون التحقيق وجوبياً في الجنايات واختيارياً في الجنح ويجوز في المخالفات، ويقوم قاضي التحقيق باتخاذ جميع الاجراءات اللازمة للكشف عن الحقيقة بالبحث والتحري عن أدلة الاتهام إلى جانب أدلة النفي كذلك، كما يقوم بعملية الانتقال للمعاينة والأمر بالتفتيش، وعملية ضبط الأشياء، واستجواب المتهم وسماع الشهود، وندب الخبراء، بالإضافة إلى البحث عن المتهم من النواحي الاجتماعية كحالته المادية أو من خلال تكليفه للضبطية القضائية القيام بذلك وغيرها من الصلاحيات المنوطة به، ويقوم قاضي التحقيق بإجراءات التحقيق الخاصة التي جاءت في قانون الاجراءات الجزائية الجزائري في المذكورة في المادة 65 مكرر5 من قانون الاجراءات الجزائية، ويختص قاضي التحقيق بعد فتح التحقيق القضائي بمنح الإذن من أجل القيام بعملية التسرب، وعمليات التقاط الصور واعتراض المراسلات وتسجيل الأصوات، ويتم الإشراف

(1) لعاقل فريال، مرجع سابق، ص 78.
(2) نبيل محمود فريد أبو الرب، مرجع سابق، ص80،ص81.

عليها من طرف وكيل الجمهورية، ويمنح قاضي التحقيق الإذن باتخاذ الإجراءات الخاصة السابقة في جرائم المخدرات، الجريمة المنظمة عبر الحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف[1]، ويختص قاضي التحقيق بممارسة صلاحياته من خلال الشكوى المصحوبة بالادعاء المدني من طرف المتضرر.

أما فيما يتعلق بالاختصاص الاقليمي فهو على نوعان إما أن يكون محلياً أو يكون وطنياً كالآتي:

1- الاختصاص المحلي لقاضي التحقيق.

يتحدد هذا الاختصاص بدائرة المحكمة او المحاكم التي يباشر قاضي التحقيق فيها وظيفته بحسب قرار تعيينه، وينعقد على هذا الاختصاص بمكان وقوع الجريمة أو محل إقامة المشتبه فيهم أو بمحل إلقاء القبض على المتهم.

2- الاختصاص الوطني لقاضي التحقيق.

هو اختصاص يشمل كامل التراب الوطني، وتم النص على هذا النوع من الاختصاص في المادة 2/40 من قانون الإجراءات الجزائية، وذلك عندما يتعلق الأمر بجريمة من جرائم الإرهاب، المخدرات، الجريمة المنظمة عبر الحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، أو الجرائم الماسة بالتشريع الخاص بالصرف[2].

أما المنظومة القانونية الفلسطينية فلا يوجد بها هذه الجهة المتمثلة بقضاة التحقيق، بحيث أن أعمال التحقيق تمارسها النيابة العامة وفق ما خوله لها قانون الاجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 من صلاحيات، وذلك في سبيل الكشف عن الحقيقة والوصول إلى مرتكبي الجرائم بأنواعها، لقد منح القانون للنيابة اتخاذ جميع اجراءات التحقيق ومنها منح الإذن بالتفتيش، وندب الخبراء والتصرف في الأشياء المضبوطة وسماع الشهود واجراء الاستجواب واصدار مذكرات الحضور والإحضار، تمديد التوقيف للنظر.

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، مصدر سابق، المواد 66، 67، 68، 65 مكرر5.

(2) منتديات ستار تايمز، القواعد العامة لنظام قاضي التحقيق، منشور بتاريخ 2009/9/20.

الفرع الخامس: القانون الواجب التطبيق.

نعالج في هذا الفرع القانون الواجب تطبيقه عند ارتكاب جريمة معلوماتية سواء وقع الفعل المجرّم وحدثت النتيجة في نفس إقليم الدولة أو تم ارتكاب الفعل الاجرامي في دولة والنتيجة وقعت في دولة أخرى.

نصّ المشرع الجزائري من خلال المادة 03 من قانون العقوبات على أنه " **يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية.**

كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية"[1].

ونص قانون العقوبات الاردني رقم 16 لسنة 1960 المطبق في الضفة الغربية في المادة 07 منه على "**1- تسري أحكام هذا القانون على كل من يرتكب داخل المملكة جريمة من الجرائم المنصوص عليها فيه.**

2- تعد الجريمة مرتكبة في المملكة، إذا تم على أرض هذه المملكة أحد العناصر التي تؤلف الجريمة أو فعل من أفعال جريمة غير متجزئة او فعل اشتراك أصلي أو فرعي.

3- تشمل أراضي المملكة طبقة الهواء التي تغطيها، والبحر الإقليمي إلى مسافة خمسة كيلومترات من الشاطئ والمدى الجوي الذي يغطي البحر الإقليمي والسفن والمركبات الهوائية الأردنية.

4- والأراضي الأجنبية التي يحتلها الجيش الأردني إذا كانت الجريمة المقترفة تنال من سلامة الجيش أو من مصالحه."[2].

كما نص قانون العقوبات رقم 74 لسنة 1936 المطبق في قطاع غزة في المادة 06 منه على " **إيفاء للغاية المقصودة من هذا القانون يتناول اختصاص محاكم فلسطين جميع أنحاء فلسطين ومسافة ثلاثة أميال بحرية من شاطئ فلسطين مقيسة من اوطى علامة للجزر**"، كما نصت المادة 07 منه على " **إذا ارتكب فعل، بعضه داخل نطاق اختصاص محاكم فلسطين وبعضه خارج نطاق اختصاصها، وكان ذلك الفعل يؤلف جرماً ينطبق على أحكام هذا القانون فيما لو ارتكب بأكمله ضمن نطاق اختصاص تلك**

---

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-156 المرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدّل والمتمم، مصدر سابق، المادة 03.

(2) دولة فلسطين، قانون العقوبات الأردني رقم 16 لسنة 1960 المطبق في الضفة الغربية، مصدر سابق، المادة 07.

المحاكم، فكل شخص ارتكب أي قسم من ذلك الفعل ضمن نطاق اختصاص محاكم فلسطين يجوز محاكمته ومعاقبته بمقتضى هذا القانون كما لو كان قد ارتكب ذلك الفعل بأكمله ضمن نطاق اختصاص تلك المحاكم."[1].

أولاً الجرائم المرتكبة داخل الإقليم.

باستقراء النصوص سالفة الذكر نرى بان كلا التشريعين الجزائري والفلسطيني عملا على تكريس نبدأ إقليمية القوانين فالإقليم يتكون من المجال البري، المجال الجوي، والمجال البحري.

ويقتضي مبدأ إقليمية القوانين أن تكون الجريمة المعلوماتية ارتكبت بكامل اركانها داخل إقليم الدولة ومن ذلك فإذا ما ارتكبت الجريمة المعلوماتية داخل إقليم الدولة الجزائرية أو الفلسطينية، فإنه يطبق عليها أحكام قانون العقوبات سواء الجزائري إذا ما ارتكبت في الجزائر، أو الفلسطيني إذا ما ارتكبت في فلسطين، وذلك في حدود ما يشمله مفهوم إقليم الدولة.

كما يمكن أن تكون أركان الجريمة المرتكبة تمت في أكثر من دولة، لكن تحديد مكان ارتكاب الجريمة ليس بالأمر السهل، فقد يقوم أحد المخترقين باستعمال جهاز كمبيوتر محمول مجهز بخدمة الإنترنت ويقوم باختراق وتخريب نظام أحد البنوك في دولة أخرى أو عدة دول في آن واحد، فما هو القانون الواجب تطبيقه في هذه الحالة؟[2].

باستطلاع قانون الاجراءات الجزائية الجزائري عالجت المادة 586 والتي مفادها أنه تعتبر الجريمة مرتكبة في الدولة الجزائرية إذا ما تم ارتكاب عمل من الاعمال المكونة للجريمة تم في الجزائر، وكذا جاءت المادة 585 منه لتدل على أن قانون العقوبات الجزائري يطبق على كل من كان في اقليم الجزائر باعتباره شريكاً في جناية أو جنحة مرتكبة في الخارج، إلا أن هذه الأحكام الواردة في المادة 585 يجب توفر شرطين لتطبيقها وهما:

1. أن يكون الفعل معاقباً عليه في الجزائر وفي الاقليم الذي ارتكب في الفعل.
2. أن تكون الواقعة تشكل جناية أو جنحة، وثبت ارتكابها بقرار نهائي من الجهة القضائية الأجنبية[3].

---

(1) دولة فلسطين، قانون العقوبات رقم 74 لسنة 1936 المطبق في قطاع غزة، مصدر سابق، المادة 06، 07.
(2) صديق حياة، مرجع سابق، ص 55.
(3) مرجع نفسه، ص55.

وباستقراء النصوص الواردة في قانون العقوبات المطبق في الضفة الغربية والقانون المطبق في قطاع غزة، نجد بأن الأحكام المتعلقة بالقانون الواجب التطبيق إذا ما ارتكبت أركان الجريمة في أكثر من دولة، فقد أجاب قانون الاجراءات الجزائية رقم 3 لسنة 2001 في المادة 166 والتي مفادها أنه في حال ارتكاب جريمة كان بعضاً منها ارتكب داخل اختصاص محاكم فلسطين والبعض الآخر ارتكب خارج نطاق اختصاصها فإنه يطبق عليه أحكام قانون العقوبات الفلسطيني كما لو أنه ارتكب الفعل بأكمله في فلسطين[1].

كما أجابت المادة 07 من قانون العقوبات رقم 74 لسنة 1936 المطبق في قطاع غزة سالفة الذكر، أنه يتم تطبيق القانون الفلسطيني في حال ما إذا ارتكبت جريمة جزءاً من اركانها ارتكب داخل فلسطين والجزء الآخر ارتكب في دولة أخرى، فإنه يتم تطبيق أحكام قانون العقوبات الفلسطيني على مرتكبها كما لو كان قد ارتكبها كاملةً في فلسطين.

وجاءت المادة 1/2 من القرار بقانون رقم 16 لسنة 2017 لتحدد القانون الواجب في حال ارتكاب جزءاً من الفعل داخل أو خارج فلسطين فيما يتعلق بالجرائم الالكترونية، فإن ذلك القرار بقانون يسري على تلك الأفعال.

وخلاصة القول أنه في حال تم ارتكاب جريمة معلوماتية وكانت أركانها ممتدة لتشمل عدة أقاليم، فإن كلا التشريعين الجزائري والفلسطيني تم النص من خلالهما على تطبيق أحكام قانون العقوبات على تلك الجريمة كما لو كانت مرتكبة بشكل تام داخل إقليم الدولة الجزائرية أو الفلسطينية.

ثانياً: الجرائم المرتكبة خارج الإقليم.

الأصل في تطبيق القانون على الجرائم المعلوماتية هو مبدأ الاقليمية، واستثناءً في حالات محددة يتم تطبيق مبدأ عينية النص الجنائي ويطبق هذا المبدأ عندما ترتكب جريمة تمس بأمن الدولة أو باقتصادها الوطني، ويطبق أيضا استثناءً مبدأ شخصية النص الجنائي، ويتم تطبيق هاتين المبدأين في حالات محددة على سبيل الحصر كالآتي:

1. في التشريع الجزائري.

أ- يتم تطبيق مبدأ عينية النص الجنائي طبقاً لنص المادة 588 من قانون الاجراءات الجزائية والذي مقتضاه تطبيق قانون العقوبات الجزائري على كل أجنبي أو جزائري يرتكب خارج إقليم الدولة الجزائرية

[1] دولة فلسطين، قانون الاجراءات الجزائية رقم 03 لسنة 2001، مصدر سابق، المادة 166.

جريمة تمس أمن الدولة الجزائرية أو تزييف النقود أو أوراق، تجوز متابعته ومحاكمته وفقاً لأحكام القانون الجزائري، ويبرر الأخذ بهذا المبدأ وجوب الدفاع عن السيادة الوطنية[1]، وبذلك يطبق قانون العقوبات الجزائري على كل اجنبي أو جزائري يرتكب جريمة معلوماتية تمس بأمن الدولة أو باقتصادها[2].

ب- ويتم تطبيق مبدأ شخصية النص الجنائي حسب المادتين 582 و 583 من قانون الاجراءات الجزائية على كل جزائري يرتكب جناية أو جنحة خارج إقليم الدولة الجزائرية، شريطة أن الواقعة المرتكبة تشكل جناية أو جنحة في التشريع الجزائري وفي تشريع الدولة التي ارتكبت فيها، أن يكون المتهم جزائرياً، أن يعود المتهم إلى الجزائر، وأن لا يكون المتهم قد حكم عليه نهائياً في الخارج فلا يجوز محاكمة الشخص على ذات الجرم مرتين[3].

2. في التشريع الفلسطيني.

أ. نصت المادة 09 من قانون العقوبات الاردني المطبق في الضفة الغربية على مبدأ عينية النص الجنائي (الصلاحية الذاتية)، بحيث تسري أحكام قانون العقوبات على كل فلسطيني أو أجنبي ارتكب خارج أراضي فلسطين جريمة من شأنها المساس بأمن الدولة أو قلد أختام الدولة أو قلد نقوداً أو زور أوراق أو السندات المصرفية الأردنية أو الأجنبية المتداولة قانوناً أو تعاملاً في الدولة، فهذا المبدأ قابل للتطبيق على الجريمة المعلوماتية التي قد يرتكبها أجنبي أو فلسطيني ارتكب جريمةً معلوماتية تمس بأمن الدولة أو باقتصادها الوطني، بحيث يتم تطبيق قانون العقوبات الفلسطيني لحماية السيادة الوطنية للحفاظ على سلامة أمنها وحماية اقتصادها[4]، فارتكاب جريمة معلوماتية من طرف أجنبي خارج إقليم دولة فلسطين وكان من شأنها المساس بأمن الدولة أو اقتصادها الوطني فإنه يسري عليه قانون العقوبات الفلسطيني.

ب. كما نصت المادة 10 من نفس القانون السابق على قابلية تطبيق مبدأ شخصية النص الجنائي، والذي مفاده سريان قانون العقوبات المطبق في الضفة الغربية على كل فلسطيني ارتكب جناية أو جنحة خارج إقليم الدولة الفلسطينية حتى ولو ارتكبها بعد فقده للجنسية أو اكتسابه لها، وتسري أحكام هذا القانون كذلك على المقيم الأجنبي الذي يرتكب جنحة او جناية في الخارج[5]، شريطة أن تكون تلك الجناية أو الجنحة معاقب عليها في كلا التشريعين الفلسطيني وتشريع الدولة التي ارتكبت فيها الجريمة، وأن يعود المتهم إلى فلسطين، وأن يكون حاملاً للجنسية الفلسطينية أو مقيماً في فلسطين، وأن لا يكون قد حكم

(1) صديق حياة، مرجع سابق، ص56.
(2) عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص51.
(3) صديق حياة، مرجع سابق نفسه، ص56.
(4) دولة فلسطين، قانون العقوبات الأردني رقم 16 لسنة 1960 المطبق في الضفة الغربية، مصدر سابق، المادة 09.
(5) دولة فلسطين، قانون العقوبات الأردني رقم 16 لسنة 1960 المطبق في الضفة الغربية، مصدر سابق، المادة 10.

عليه بحكم نهائي بات في الدولة التي ارتكب بها الجريمة، حيث لا يعاقب الشخص على ذات الجرم مرتين. ومن ذلك فإن الفلسطيني أو المقيم الذي يرتكب جريمة معلوماتية خارج إقليم دولة فلسطين وتوفرت فيه الشروط المذكورة سابقاً، فإنه يعاقب وفقاً لأحكام قانون العقوبات الفلسطيني.

وتجدر الإشارة إلى أن تم النص على مبدأ شخصية القانون وكذا مبدأ العينية في القرار بقانون رقم 16 لسنة 2017 من خلال المادة في المادة 2/2 بحيث اشتملت على نفس الشروط، ولكن جاء ذلك لكي يحيط الجريمة المعلوماتية بمعاملة ردعية خاصة.

المطلب الثاني: أعمال التحقيق.

بالنظر للتطور السريع الذي تعرفه الجريمة المعلوماتية، ومن اجل مكافحتها مكافحة ناجعة، قام كلا المشرعين الجزائري والفلسطيني باستحداث إجراءات خاصة، من أجل الكشف عن تلك الجرائم المعلوماتية، وتوقيع العقاب على مرتكبيها كان لابدّ من إجراءات تساير الطبيعة الخاصة لتلك الجريمة.

سنتطرق لدراسة الإجراءات الخاصة المتعلقة بالجريمة المعلوماتية وضوابطها، والخصوصية التي تتمتع بها تلك الإجراءات إذا ما اتُخِذَت بصدد جريمة معلوماتية، وسنتناول بالدراسة، التسرب، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

الفرع الأول: التسرب.

هو الإجراء المستحدث في قانون الاجراءات الجزائية الجزائري ونصت عليه المواد من 65 مكرر11 إلى 65 مكرر18، وجاء تعريف هذا الإجراء في المادة 65 مكرر12 على أنه " **قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية او جنحة، بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف**" ويتخذ هذا الإجراء في إطار جرائم محددة على سبيل الحصر في المادة 65 مكرر5 والتي من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[1].

ويتميز إجراء التسرب بنوع من الخطورة، حيث يقوم الضابط أو العون المكلف بالعملية باختراق الوسط الإجرامي المغلق أي الجماعة الإجرامية بهدف الحصول على معلومات تفيد في كشف الحقيقة عن

[1] الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون الإجراءات الجزائية، مصدر سابق، المواد65 مكرر 12، 65 مكرر5.

الجرائم ومرتكبيها، بحيث يعمل تحت تغطية قانونية أي أنه لا يظهر هويته الحقيقة، وأيضاً بهدف كسب ثقة الجماعة الإجرامية[1].

وقد أورد المشرع الجزائري جملة من الشروط لا بد من توافرها لصحة إجراءات التسرب وهي:

- أن يكون هناك إذن مكتوب ومسبب موجه من وكيل الجمهورية أو قاض التحقيق.
- أن يوجه هذا الإذن إلى ضباط الشرطة القضائية أو أعوانه تحت مسؤولية ضابط الشرطة القضائية[2].
- تحديد مدة التسرب ب 04 أشهر قابلة للتجديد.
- أن ينصب الإذن على الجرائم المستحدثة والمحددة قانوناً.
- تحديد هوية ضابط الشرطة القضائية التي تتم عملية التسرب تحت مسؤوليته.
- جواز إيقاف عملية التسرب قبل انقضاء المدة المحددة.
- إدراج الإذن في ملف الإجراء بعد الانتهاء من عملية التسرب، يمنح الإذن وكيل الجمهورية أو قاضي التحقيق المكلف بالملف بعد إخطار النيابة العامة ويتم تحت رقابة القاض الآمر به، مع التقيد بالشروط السابقة تحت طائلة البطلان[3].

ومن ذلك نرى بأن عملية التسرب هي عملية جداً خطيرة، كونها تستوجب انخراط عون أو ضابط الشرطة القضائية في إطار جماعة اجرامية تمارس الاجرام المعلوماتي، وذلك عن طريق إيهامهم بأنه فاعل أو شريك لهم أو خافِ، فقد يقوم العون أو الضابط المتسرب بارتكاب الجرائم المعلوماتية إلا أن ذلك غير مبني على إرادة آثمة وخطورة إجرامية، فارتكابه للجرائم المعلوماتية يكون بهدف الايقاع بمكن يرتكبوها بإيهامهم بأنه شريكاً أو فاعلاً أو خافِ.

وبعد انتهاء عملية التسرب تتمكن جهات البحث والتحري وعلى رأسها وكيل الجمهورية وقاضي التحقيق من الوقوف على التفاصيل الأساسية لارتكاب الجرائم لا سيما الجرائم المعلوماتية، وكذا تحرير المحاضر التي تخدم الدعوى وتعطي نظرة عميقة لحقيقة ما يحدث في بؤر الإجرام وداخل العصابات، كما تطرح أمام جهات الحكم بما لها من حرية في تقدير ما يعرض عليها من أدلة والتي من ضمنها المحاضر المحررة حسب الأشكال القانونية المقررة لها، وكل مخالفة تبطل ما يترتب عنها، كما تقدم للقاضي

(1) قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في القانون تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند اولحاج البويرة، 2015.

(2) بوعوينة أمين شعيب، مهلب حمزة، اختصاصات لضبطية القضائية في القانون الجزائري، مذكرو لنيل شهادة الماستر في الحقوق شعبة القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة بجاية، 2013/2012.

(3) عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2014/2013.

الفاصل في الدعوى شهادات لشهود عيان خاطروا بأنفسهم للحصول على الدليل، وهذا كله لتحقيق الهدف الأساسي من الدعوى العمومية تحديداً والإثبات الجنائي عموماً في البحث عن الحقيقة والكشف عنها[1].

أما قانون الإجراءات الجزائية الفلسطيني فلم ينص على هكذا إجراء، فاكتفي بالوسائل التقليدية للإثبات، لا سيما فيما يتعلق بإجراء التسرب، فباستقراء نصوص القانون نجد أن اختصاصات النيابة العامة تنحصر في جمع الادلة من خلال التفتيش والضبط وغيرها من الاجراءات المنصوص عليها في قانون الاجراءات الفلسطيني رقم 03 لسنة 2001 بحيث يتم اتخاذ تلك الاجراءات في سبيل الكشف عن الحقيقة والوصول إلى مرتكب الجريمة.

الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

لقد نص المشرع الجزائري في قانون الاجراءات الجزائية الجزائري في المواد من65 مكرر5 إلى 65 مكرر10 على إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

أولاً: اعتراض المراسلات وتسجيل الأصوات.

يقصد باعتراض المراسلات التتبع السري والمتواصل للمشتبه به قبل وبعد ارتكاب الجريمة ثم القبض عليه متلبساً بها، ويعرف على أنه إجراء تحقيقي يباشر خلسةً وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، أما تسجيل الأصوات فهو النقل المباشر والآلي للموجات الصوتية من مصادرها بنبراتها ومميزاتها الفردية وخواصها الذاتية، بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه، و تعتبر أيضاً وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية في مواجهة الإجرام الخطير بشكل عام والجرائم المعلوماتية بشكل خاص وتتم عبر وسائل الاتصال السلكية واللاسلكية[2].

---

(1) زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد الحادي عشر، 2014، ص8.

(2) قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لمتطلبات شهادة الماستر أكاديمي تخصص قانون عام للأعمال، جامعة قاصدي مرباح ورقلة، السنة الدراسية 2013-2014، ص32.

وبخصوص اتخاذ هذا الإجراء بصدد الجرائم المعلوماتية فإنه يتمثل باعتراض المراسلات وتسجيل الأصوات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وذلك بواسطة ترتيبات تقنية يتم وضعها ودون موافقة المعنيين، وتتخذ من أجل ما يلي:

3- التنصت والتقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية.

فالواضح أن هذه التدابير وضعت بشكل محكم ومرتب يهدف في النهاية إلى رصد الدليل الذي سوف يثقل كاهل المجرم المعلوماتي إذا خص الإجراءات في هذا النوع من الجرائم وجرائم أخرى محددة، فالملاحظ أن هذه الترتيبات التقنية يتم وضعها دون علم المعنيين ودون موافقة مسبقة من هؤلاء المعنيين بالمراقبة[1].

ومن خلال تلك الاجراءات يتم رصد كل كلمة وكل المحادثات التي تجري بين هؤلاء وهذا الكلام أو المحادثات الملتقطة يتم تثبيتها بتسجيلها وبثها عند الحاجة ومن ثم يستعمل كدليل يواجه به المتهم، ويستوي في ذلك أن يكون الكلام بصفة خاصة أو سري وسواء من طرف شخص صادر منه لجهة أخرى بين عدة اشخاص وفي اماكن خاصة أو عمومية[2].

وتجدر الإشارة إلى اعتراض البريد الإلكتروني والذي يعتبر من أهم الوسائل الحديثة للاتصال في مجال الانترنت وهو اكثر استخداماً في هذا المجال نظراً لما يتسم به من سرعة وسهولة في الاستخدام، ويشكل البريد الالكتروني حالياً طبقة من المواطنين على مستوى جميع الدول وهو ما يصطلح عليه المواطنون الرقميون، ولذلك فهو يتمتع بالحماية القانونية وهو ما نص عليه المشرع الجزائري في المادة 65 مكرر5 من قانون الإجراءات الجزائية بأن جعل من اختصاص القضاء في مجال الجرائم المعلوماتية بأن يأذن وكيل الجمهورية في إطار التحري والتحقيق الابتدائي باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية التي يندرج ضمنها البريد الإلكتروني وأذن القانون بوضع الترتيبات التقنية اللازمة لاعتراض البريد الالكتروني- بحسب رأي الأستاذ زبيحة زيدان -، حيث أن البريد الالكتروني يعتبر بيئة خصبة للإجرام المعلوماتي ولم يسلم من الاقتحام من قبل مجرمي المعلوماتية [3].

(1) زبيحة زيدان، مرجع سابق، ص157.
(2) زيدان، مرجع نفسه، ص 158.
(3) زبيحة زيدان، مرجع سابق، ص160.

أما المشرع الفلسطيني ينص في قانون الاجراءات الجزائية رقم03 لسنة 2001 على إجراء اعتراض المراسلات وتسجيل الأصوات، لا سيما المادة 51 من القانون السابق، حيث خول النيابة العامة في إطار ممارسة التحقيقات عن الجنايات والجنح التي تكون عقوبتها لا تقل عن سنة واحدة، شريطة أن يكون هناك إذن صادر عن قاضي الصلح المختص، ومن ذلك نرى بأن المشرع الفلسطيني ينص على هذا الإجراء في كل الجرائم التي تكون عقوبتها لا تقل عن سنة واحدة على عكس المشرع الجزائري الذي اشترطها في جرائم محددة على سبيل الحصر، فنرى بأنه في يمكن للنيابة العامة اتخاذ إجراء اعتراض المراسلات وتسجيل الأصوات في إطار التحقيق عن الجرائم المعلوماتية.

ثانياً: التقاط الصور.

هي احدى الوسائل الحديثة التي يستخدمها المشرع الجزائري لمكافحة الاجرام المعلوماتي، هي في حقيقة الأمر استثناء عن الأصل العام الذي يمنع التقاط الصور باعتباره تدخل في الحياة الخاصة.

أدى تطور الجريمة وازدياد معدلاتها من خلال استخدام المجرمين لأحدث الأساليب العلمية في ارتكابهم للجرائم إلى ضرورة البحث عن الحلول التي تحد من تفاقم معدلات الجريمة واذا استمر التطور التقني في إنتاج اجهزة التصوير وزيادة كفاءة العدسات التلسكوبية والأفلام واختراع الدوائر التلفزيونية المغلقة التي تسمح بمراقبة مكان ما ومعرفة كل ما يدور بداخله دون علم الحاضرين[1].

وهذا الإجراء يقوم أساساً على استخدام الكاميرات أو أجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة اشخاص مشتبه في أمرهم، على الحالة التي كانوا عليها وقت التصوير لغرض استخدام محتوى الفيلم كمادة إثبات ودليل مادي أو بمعنى آخر مادة مرئية في المحاكم لضمان اتخاذ الإجراءات الوقائية لضبط المجرمين أو المشتبه فيهم، وهذا الإجراء يربط الأشخاص في زمان ومكان وفي وقت واحد، وخاصة مع التطور التكنولوجي والعلمي أصبح بإمكان استخدام وسائل حديثة وذات تقنية جيدة تساعد على التقاط الصور بجودة عالية، وهناك أجهزة تعمل بالأشعة تحت الحمراء تلتقط صور الأشخاص ليلاً، حيث تستخدم هذه الاجهزة لنقل الصوت والصورة للمجرم المعلوماتي بشكل لا يلفت الانتباه، مما يمكن ضابط الشرطة القضائية من سماع ورؤية ما يدور في حياة المشتبه فيه طوال مدة البحث والتحري[2].

---

(1) عباسي خولة، مرجع سابق، ص44.

(2) قادري سارة، مرجع سابق، ص38،ص39.

ومن خلالها يلتزم ضابط الشرطة القضائية بتحرير محضر عن العملية التي قام بها وتسجيل تاريخ وساعة بدايتها ونهايتها د، كما يتعين عليه أن يصف الصور الملتقطة في محضر يودع بملف الاجراءات الخاص بالدعوى وذلك حسب نص المادة 65مكرر 9 و65 مكرر 10 من قانون الإجراءات الجزائية الجزائري[1].

بالنسبة لموقف المشرع الفلسطيني من إجراء التقاط الصور ، فقانون الإجراءات الجزائية الفلسطيني لم يمنح النيابة العامة ذلك الإجراء في إطار التحقيق عن الجرائم بشكل عام، ولكن القرار بقانون المتعلق بالجرائم الالكترونية جاء بإجراءات خاصة سنتناولها لاحقاً.

ثالثاً: الشروط الخاصة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

1. يجب أن يصدر الإذن مكتوباً من وكيل الجمهورية في مرحلة التحقيق الابتدائي، ويصدر من قاضي التحقيق في حالة فتح التحقيق القضائي بحسب المادة 65 مكرر 5 من قانون الاجراءات الجزائية الجزائري.

ويجب أن يصدر الإذن من طرف قاضي الصلح المختص وذلك حسب نص المادة 2/51 من قانون الاجراءات الجزائية الفلسطيني.

2. يجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غير سكنية ونوع الجريمة التي تطلبت استعمال هذه التدابير بحسب ما جاء في المادة 65 مكرر 7 من قانون الإجراءات الجزائية الجزائري.

يجب أن يتضمن الأذن الصادر عن قاضي الصلح نوع الجريمة المطلوب اتخاذ اجراء اعتراض المراسلات وتسجيل الأصوات بصددها، وأن يكون مسبباً، كما يمكن أن يتخذ في الأماكن الخاصة وذلك بحسب ما جاء في المادة 2/51 من قانون الإجراءات الجزائية الفلسطيني.

3. تكون مدة الإذن 4 أشهر قابلة للتجديد حسب مقتضيات البحث والتحري بحسب المادة 65 مكرر 7 من قانون الإجراءات الجزائية الجزائري[2].

وتكون مدة الإذن لا تتجاوز 15 يوماً قابلة للتجديد مرة واحدة حسب ما جاء في المادة 3/51 من قانون الإجراءات الجزائية الفلسطيني[3].

---

(1) قادري سارة، مرجع سابق،، ص39.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، مصدر سابق، المواد 65 مكرر5- 65 مكرر7.

(3) دولة فلسطين، قانون الإجراءات الجزائية رقم 03 لسنة 2001، مصدر سابق، المادة 51.

فإجراء التسرب مهما كانت الجماعة الإجرامية ذكيةً في طمس أي دليل من الممكن أن تخلفه وراءها فإنه عند اختراقها من طرف أحد ضباط أو أعوان الشرطة القضائية وقيامه بإيهامهم بأنه معهم، وقيامهم بارتكاب الجريمة سيؤدي إلى إلقاء القبض عليهم في حالة تلبس أو الوصول إلى أماكنهم.

وإجراء اعتراض المراسلات وتسجيل الأصوات، والذي من حق أي شخص أن يتمتع بسرية المراسلات كحق دستوري، إلا أنه يمكن ان يتم اعتراض تلك المراسلات طالما كانت تنطوي على ارتكاب جريمة ما لا سيما إذا كانت جريمة معلوماتية، وبالإمكان تسجيل صوت المعني بالمراقبة وتثبيت كل الكلام الذي يتفوه به على أشرطة مغناطيسية يمكن إعادة سماعها، الأمر الذي يجعل منها دليلاً مادياً على إثبات التهم المنسوب للمتهم أو لإثبات تورط شخص آخر مشتبه به بارتكاب جريمة معلوماتية.

وعملية التقاط الصور تؤدي حتماً إلى تبيان مرتكب الجريمة وكذا ماديات الجريمة ومكان ارتكابها، فيمكن أن يتم تصوير أحد القراصنة أثناء قيامه بعملية الدخول غير المشروع إلى نظام معالجة، فإذا ما كانت تلك الصور الملتقطة، تمت وفق الشروط القانونية المرسومة لها فإنها تشكل دليلاً على مرتكب الجريمة أثناء تقديمه للمحاكمة بعد إلقاء القبض عليه.

وتتخذ هذه الإجراءات إلى جانب الإجراءات التقليدية في البحث والتحري، لكي تكون مكملة لبعضها البعض وتعطي صورة متكاملة عن الجريمة المرتكبة أو لتسهيل الوصول إلى مرتكبيها في حال ما استعصي إثباتها بالوسائل التقليدية.

ومن الوسائل التقليدية المتبعة في البحث والتحري عن الجرائم لا سيما الجرائم المعلوماتية هي الاستجواب، معاينة مسرح الجريمة، سماع الشهود، والضبط وما إلى ذلك من إجراءات البحث والتحري التي تتخذها النيابة العامة والضبطية القضائية من أجل الكشف عن الحقيقة والقبض على مرتكبي الجرائم المعلوماتية.

وهذه الإجراءات هي التي نصّ عليها قانون الإجراءات الجزائية والتي تتمتع بنوع من الخصوصية لخطورتها ومساسها بالحقوق والحريات، إلا أن كلا المشرعين الجزائري والفلسطيني جاءوا بإجراءات خاصة بالبحث والتحري عن الجرائم المعلوماتية وذلك من خلال القوانين الخاصة المتعلقة بهذا النوع من الجرائم لا سيما القانون الجزائري رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني، فكلا القانونين اشتملا على إجراءات خاصة بالجرائم المعلوماتية وهو ما سنفصّل فيه في المبحث الثاني.

وخلاصة القول بأن كلا المشرعين الجزائري والفلسطيني جاءوا بأساليب خاصة بالبحث والتحري عن الجرائم بشكل عام، وعن الجرائم المعلوماتية بشكل خاص، فالخطورة الإجرامية لمرتكب الجريمة المعلوماتية والذكاء الذي يتمتع به للحيلولة دون وقوعه في قبضة العدالة دفعت بكلا المشرعين إلى اتخاذ إجراءات استثنائية، تدفعنا إلى القول بأنها قد تنتهك حقوق وحريات الأفراد، إلا أن المحافظة على النظام العام، وحماية لمجتمع من الظواهر الإجرامية، لا سيما ظاهرة الإجرام المعلوماتي.

المبحث الثاني

المكافحة الإجرائية للجريمة المعلوماتية في ظل القوانين الخاصة

لقد صدر في أعقاب تعديل قانون العقوبات الجزائري القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وبعد الفراغ التشريعي في التشريع الفلسطيني فيما يتعلق بمكافحة ظاهرة الإجرام المعلوماتي صدر القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية ليكافح هذا النوع من الجرائم وكذا النص على إجراءات خاصة تتخذ في إطار البحث والتحري عن الجرائم المعلوماتية.

كما نص كلا القانونين على مكافحة الإجرام المعلوماتي وذلك من خلال إنشاء هيئات متخصصة لتكافح وتتابع هذا النوع من الجرائم بناءً على تنظيم وبناء قانوني معين لتلك الهيئات القائمة على محاربة الجريمة المعلوماتية بكافة أشكالها.

وسنفصل في هذه الإجراءات بحيث سنتناول في المطلب الأول أعمال التحقيق الخاصة، والمطلب الثاني: إنشاء هيئات متخصصة.

المطلب الأول: أعمال التحقيق الخاصة

لقد جاء كلا القانونين 09-04 الجزائري والقرار بقانون رقم 16 لسنة 2017 الفلسطيني بإجراءات خاصة لمكافحة الجريمة المعلوماتية، وكلا القانونين كانت لهما رؤية في التصدي لهذا النوع من الجرائم، فهناك من الإجراءات ما هو مشترك بينهما وهناك ما نصّ عليه القرار بقانون رقم 16 لسنة 2017 ولم ينص عليه القانون 09-04، وعليه سنقسم هذا المطلب إلى فرعين الأول يتعلق بالإجراءات المشتركة بين القانونين، والثاني يتعلق بالأحكام المختلفة بين القانونين.

الفرع الأول: أعمال التحقيق المشتركة بين القانون الجزائري المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال والقرار بقانون بشأن الجرائم الإلكترونية.

كما أسلفنا بأن القانون رقم 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال جاء بإجراءات نصّ عليها كذلك القرار بقانون رقم 16 لسنة 2017، وتتمثل هذه الإجراءات المشتركة في التفتيش، مراقبة الاتصالات الإلكترونية، والضبط.

أولاً: التفتيش.

تهدف وسائل الإثبات الجنائي جميعاً إلى الوصول على دليل لكشف الحقيقة، لكن التفتيش يتميز عن بعضها بان ما يهدف الوصول إليه وضبطه هو دليل مادي للجريمة، فشهادة الشهود، الاستجواب، والاعتراف، قد توصل إلى أدلة تكشف عن الحقيقة ولكنها ادلة قولية، إلا أن ثمة وسائل بحث قانونية أخرى توصل إلى دليل أو أدلة مادية كالمعاينة، الخبرة، والتفتيش [1].

باعتبار أن التفتيش، إجراء من إجراءات التحقيق الابتدائي، فهو يخضع لسائر الأحكام التي تحكم التحقيق الابتدائي سواء وجوب تدوينها أو سريتها على الجمهور، وجواز اتخاذها في غيبة الخصوم ووكلائهم ، وهو ليس من إجراءات التحقيق النهائي التي يجوز للمحكمة أن تقوم بها في لا تملك الحق بالقيام بهذا الإجراء[2].

1. الطبيعة القانونية للتفتيش الإلكتروني.

تفتيش نظم الحاسوب والإنترنت يمكن تعريفه بأنه " **البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه**"[3].

وتفتيش نظم الحاسوب والانترنت عند ارتكاب جريمة معلوماتية، يتميز بطبيعة قانونية خاصة، ويختلف التفتيش عندما يتعلق التفتيش بالمكونات المادية للحاسب الآلي وكذا عندما يتعلق بالمكونات المنطقية وأيضاً إمكانية تفتيش شبكات الحاسب الآلي، وهو ما سنفصل فيه على النحو الآتي:

أ. تفتيش المكونات المادية للكمبيوتر.

تخضع عملية تفتيش المكونات المادية للكمبيوتر لنفس القواعد والإجراءات القانونية المرسومة له في قانون الإجراءات الجزائية إذا ما تعلقت بجريمة معلوماتية بهدف الكشف عن الحقيقة والوصول لمرتكبها، ولكن يتوقف جواز تفتيش تلك المكونات على المكان التي تكون موجودة به، بحيث إذا كانت في مكان خاص كمسكن المتهم فلا يجوز تفتيشها إلا طبقاً للقواعد الخاصة بإجراء التفتيش طبقاً لما هو منصوص عليه في قانون الإجراءات الجزائية في كلا التشريعين، كما يجب التمييز بين ما إذا كانت تلك المكونات المادية

---

(1) مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، بدون رقم طبعة، مطابع الشرطة للنشر، مصر، 2009، ص189.

(2) عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص356.

(3) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت دراسة مقارنة، أطروحة قدمت استكمالاً لمتطلبات منح الدكتوراه فلسفة تخصص القانون الجنائي، جامعة عمان العربية، الأردن، 2003، ص21.

متصلة بكمبيوتر أخر أو بنهاية طرفية أخرى في مسكن آخر غير مسكن المتهم، ففي هذه الحالة يجب مراعاة الضمانات المقررة لتفتيش تلك الأماكن[1] بناء على ما جاء في كلا التشريعين الجزائري والفلسطيني.

ب. تفتيش المكونات المنطقية للكمبيوتر.

ثار جدل فقهي حول تفتيش مكونات الكمبيوتر المنطقية أو المعنوية، بحيث يذهب رأي من الفقه إلى القول بأنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية والتي تؤدي إلى كشف الحقيقة فإن مفهوم التفتيش يشمل البيانات الإلكترونية مهما كان شكلها وقد ساند هذا الرأي القانون اليوناني والذي يعطي الحق بتفتيش أي شيء من شانه الحصول على الدليل من خلال المادة 251، وفسر الفقه اليوناني كلمة أي شيء بأنها تشمل البيانات المنطقية والمعلومات المعالجة والمخزنة إلكترونياً.

وهناك جانب من الفقه يرى عكس ذلك، وأسسوا ذلك بناء على أن عملية التفتيش مفادها ضبط الأدلة المادية، فهذا المفهوم المادي لا يمكن أن ينطبق على البيانات المنطقية للكمبيوتر كونها غير محسوسة، واقترح هذا الرأي أن يضاف لعملية التفتيش عبارة " البيانات المعالجة عن طريق الكمبيوتر أو بيانات الكمبيوتر" وبذلك سد القصور التشريعي إزاء عملية تفتيش المكونات المنطقية للكمبيوتر[2].

ج. تفتيش شبكات الكمبيوتر.

بحيث يثار التساؤل حول مدى خضوع شبكات الكمبيوتر للتفتيش؟، واختلف الفقه في تحديد تلك الطبيعة القانونية للتفتيش في مجال الجريمة المعلوماتية إلى 3 آراء كالآتي:

- يرى أنصار هذا الرأي أن يكون حاسب المتهم متصلاً بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة، ويرى الفقه الألماني في هذه الحالة يمكن أن يمتد التفتيش إلى سجلات البيانات التي تكون في موقع آخر، بالإضافة إلى ذلك فإن مشروع قانون الحاسب الآلي في هولندا نص على جواز تمديد تفتيش نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة[3].

---

(1) إحسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، أطروحة دكتوراه في الحقوق، جامعة الجزائر1، الجزائر، السنة الجامعية 2013-2014، ص224.

(2) مرجع نفسه، ص225.

(3) عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص381.

- وهناك رأي آخر يرى بأن اتصال الحاسب الآلي بحاسب او نهاية طرفية موجودة خارج الدولة، بحيث يقوم مجرمي المعلوماتية بوضع بياناتهم خارج الدولة وذلك لعرقلة الوصول إليها والحصول على الدليل من طرف السلطات المختصة ، ولمواجهة هذا الاحتمال قد ينص المشرع على استكمال إجراءات التفتيش متى كانت لازمة تلك البيانات لتكوين الدليل حتى ولو كانت في دولة أخرى وهو ما جاء به مشروع قانون جريمة الحاسب الآلي الهولندي في مادته 125، ويمكن التصدي لهذا الاحتمال من خلال التواصل مع الدول الأخرى لتسليم تلك البيانات المخزنة داخل دولتهم عندما يكون لها ارتباط بجريمة ارتكبت في الدولة التي طلبت البيانات وهو ما قامت به اليابان بصدد جرائم ارتكبت ضد مواقع خاصة بالحكومة اليابانية، فقامت بالتواصل مع الصين والولايات المتحدة الأمريكية للحصول على معلومات مخزنة على أجهزة كمبيوتر كانت قد استخدمت في ارتكاب الجريمة[1].
- ويرى جانب آخر من الفقه بأنه يقوم على أساس السماح بالتنصب وغيرها من أشكال المراقبة التليفونية في عديد من الدول، كالقانون الفرنسي الذي يجيز اعتراض الاتصالات البعيدة وشبكات تبادل المعلومات، وفي هولندا يمكن للقاضي أن يأمر بالتنصت على شبكات اتصالات الكمبيوتر. وفي الولايات المتحدة الامريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الكمبيوتر شريطة الحصول على إذن تفتيش صادر عن القاضي، ومن ذلك يمكن تفتيش شبكات الاتصال الإلكترونية والأمر سيان لخطوط الهاتف للمراقبة والتنصت، بشرط أن تكون الدعوى العمومية قد تحركت وأن تكون تلك الصلاحيات مقتصرة على جهات الادعاء العام[2].

ويتضح لنا موقف المشرع الجزائري والفلسطيني من الآراء السابقة بانها سمحت بإجراءات المراقبة الالكترونية وكذا مراقبة الاتصالات وذلك من خلال المواد 35 و37 من القرار بقانون بشأن الجرائم الإلكترونية الفلسطيني، والمادة 4 من القانون المتعلق بالوقاية من جرائم الإعلام والاتصال الجزائري، مما يجعل تلك المعلومات التي يتم تناقلها محلاً للتفتيش في أي وقت وذلك وفقاً للشروط القانونية التي ذكرها كلا المشرعين في القانون، وكذا نص المشرع الجزائري في نفس القانون على إمكانية تمديد تفتيش منظومة معلوماتية إذا كان يمكن الدخول إليها من حاسب المتهم، وإذا لا يمكن الدخول إليها من حاسب المتهم فأنه تتم عملية التفتيش بناءً على مساعدة السلطات الأجنبية وفقاً لمبدأ المعاملة بالمثل، أما المشرع الفلسطيني فنص من خلال المادة 33 من القرار بقانون سابق الذكر بأنه تتم عمليات التفتيش للأشخاص والاماكن ووسائل المعلوماتية التي تكون متصلة بالجريمة فلم يحدد المشرع الفلسطيني موقفه من تمديد التفتيش اذا

(1) حجازي، مرجع سابق، ص381- ص383.
(2) إحسان طبال، مرجع سابق، ص327.

ما كان بالإمكان التفتيش من حاسب المتهم حاسب آخر، ونص على مسألة التعاون مع السلطات الأجنبية في إطار عملية التفتيش وفقاً لمبدأ المعاملة بالمثل.

2. محل التفتيش في الجريمة المعلوماتية.

يقصد بمحل التفتيش مستودع سر الإنسان، ومحل التفتيش في الجريمة المعلوماتية حدده المشرع الجزائري في القانون 09-04 في المادة 05 منه ويتمثل المحل بالمنظومة المعلوماتية أو جزء منها أو المعطيات المخزنة فيها وهذا بحسب الفقرة (أ) من المادة 05، كما يكون المحل منظومة تخزين المعلومات وهذا حسب الفقرة (ب) من المادة السابقة، وفي كلا الحالتين فإن محل التفتيش يكون أشياء غير مادية وهي المعلومات المخزنة داخل النظام المعلوماتي[1].

أما المشرع الفلسطيني من خلال القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية لا سيما المادة 33 والتي نصت على التفتيش، بحيث يتضح لنا محل التفتيش في الجريمة المعلوماتية والذي يتمثل في الأشخاص وكذا الأماكن التي تتواجد بها تلك الأجهزة المعلوماتية، ووسائل تكنولوجيا المعلومات وهذا بحسب الفقرة الأولى من المادة السابقة، أما الفقرة الرابعة فقد نصت على تفتيش نظام المعلوماتية الذي يتم تخزين البيانات والمعلومات بداخله وذلك من خلال قيام الخبير الإلكتروني بتفتيش النظام بعد أن يأذن له النائب العام بذلك.

وعلى الرغم من وجوبية تحديد وتعيين محل التفتيش في الجرائم التقليدية، إلا أنه في الجريمة المعلوماتية يصعب تحديد المحل، بحيث يتم تعيين المنظومة المعلوماتية كحاسوب شخص معين، إلا أنه يصعب تحديد المعلومات المخزنة فيها ويرجع ذلك إلى تداخل المعلومات والملفات التي تحتوي على هذه المعلومات وصعوبة فصلها عن بعضها البعض، كما أن صاحب النظام المعلوماتي قدي يعطي لملفاته أسماء لا تدل على محتواها ولذلك لو نطبق القاعدة العامة التي تقضي تعيين المحل فإننا نجد صعوبات كبيرة في ذلك[2].

والملاحظ ان كلا المشرعين الجزائري في القانون 09-04 والفلسطيني في القرار بقانون رقم 16 لسنة 2017، لم يشترطا تعيين المحل عند القيام بعملية التفتيش بصدد جريمة معلوماتية، فقد حدد كلاهما المحل بالنظام المعلوماتي أو الأشخاص أو الأماكن أو وسائل تكنولوجيا المعلومات التي تسخر من أجل ارتكاب الجريمة المعلوماتية.

---

(1) قريم سكورة، مرجع سابق، ص58.
(2) مرجع نفسه، ص58.

3. شروط إجراء التفتيش.

بحسب ما جاء في التشريع الجزائري لا سيما القانون 09-04 فإن تفتيش النظم المعلوماتية يخضع لنفس الشروط المنصوص عليها في قانون الإجراءات الجزائية الجزائري، والتي وردت في المادة 44 منه وهي كالآتي:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.
- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.
- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.
- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.
- في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته[1].

أما المشرع الفلسطيني فقد نص على شروط تفتيش النظم المعلوماتية من خلال المادة 33 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية وهي كالآتي:

- صدور أمر مكتوب من النيابة العامة.
- يجب أن يكون الأمر مسبباً ومحدداً.
- يمكن تجديد أمر التفتيش أكثر من مرة حسب مقتضيات التحقيق.
- يشترط أن يكون مأمور الضبط القضائي مؤهلاً للتعامل مع الجرائم الإلكترونية[2].

الفرع الثاني: مراقبة الاتصالات الإلكترونية.

يقصد بمراقبة الاتصالات: استراق السمع وتسجيل أو نقل المحادثات وذلك بدون رضاء صاحبها، وهي وسيلة يستعان بها للبحث والتحري في الجرائم المستحدثة من بينها الجرائم المعلوماتية، وقد عرّف الفقه مراقبة الاتصالات الإلكترونية بأنه وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يباشره مراقب إلكتروني خلسةً عن صاحب الاتصال، وذلك بهدف الوصول إلى أدلة تكون في شكل معلومات متحركة قبل التقاطها وتسجيلها، مستخدماً في ذلك

(1) زبيحة زيدان، مرجع سابق، ص134.
(2) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، مصدر سابق، المادة 33.

التقنية الإلكترونية كأن يقوم بإعداد صندوق بريد إلكتروني مستنسخ لمراقبة المشتبه فيه عند إرساله أو استقباله صوراً وكتابات وغيرها[1].

أولاً: التقنيات المستخدمة في مراقبة الاتصالات الإلكترونية.

سنتناول 3 أنواع من التقنيات المستخدمة في مراقبة الاتصالات الإلكترونية على سبيل المثال وهي :

1. تقنية برنامج كارنيفور.

طورت هذه التقنية إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفدرالية (FBI)، بهدف تعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بتوفير الانترنت، ويشتبه في أن الرسائل التي تمر عبر شبكاتها من خلال تقديمها للخدمات يحمل معلومات عن جرائم جنائية، وحققت هذه التقنية نجاح كبير في تعقب المجرمين، وأصبح يطلق عليها بعد 11 سبتمبر 2001 تقنية(DCS1000)، وأصبحت تستخدم للتصدي لأي محاولة لتنفيذ هجومات داخل الولايات المتحدة الأمريكية[2].

2. تقنية كشف وجمع الأدلة والقرائن من رسائل البريد الإلكتروني.

أسس جون جيسين الأمريكي سنة 1988 شركة اكتشاف الأدلة أو القرائن الإلكترونية، وهي شركة تختص بالبحث والتحري عن الوثائق الإلكترونية باعتبار أن هذه الأخيرة تترك إثاراً لا تمحى ويمكن استعادتها مهما اجتهد الفاعل في محوها، ثم طورت هذه الشركة العديد من البرامج للبحث في ذاكرة الكمبيوتر والرسائل الممحاة والمعلومات المصاحبة لها والتي لا يراها الفاعل، هذه المعلومات تشمل الطريق الذي سلكته الرسائل من الجهاز المرسل والأجهزة التي مرت بها إلى غاية وصولها إلى الجهاز المرسل إليه[3].

3. تقنية مراقبة البريد الإلكتروني.

هذه التقنية هي عبارة عن برنامج صممه الأمريكي ريتشارد أتوني، من أجل معرفة محتوى البريد الإلكتروني الموضوع تحت المراقبة، وقراءة الرسائل التي قام صاحبها بإتلافها أو محوها أو حتى تلك

(1) قريم سكورة، مرجع سابق، ص 14.
(2) مرجع نفسه، ص15.
(3) مرجع نفسه ، ص15.

المعلومات والرسائل التي لم يقم بتخزينها، فهذه التقنية تعمل على تبيان وكشف محتوى تلك الرسائل والمعلومات[1].

ثانياً: حالات اللجوء إلى مراقبة الاتصالات الإلكترونية.

حدد المشرع الجزائري الحالات التي يتم بها اللجوء إلى هذا الإجراء وقد وردت هذه الحالات على سبيل الحصر في القانون 09-04 في المادة 04 منه وهي:

- للوقاية من الأفعال الموصوفة بجرائكم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معالجة معلوماتية على نحو يهدد النظام العام أو الدفع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

ونرى بأن المشرع قد اشترط للقيام بهذه العملية لا بدّ من توفر الإذن المكتوب من وكيل الجمهورية أو من قاضي التحقيق في مرحلة التحقيق القضائي، كون أن هذا الإجراء يمس بحرية الحياة الخاصة للأفراد وخصوصيتها وهي مقدسة ومحمية دستورياً [2].

أما المشرع الفلسطيني فلم يحصر نطاق هذا الإجراء، فالمادة 35 من القرار بقانون رقم 16 لسنة 2017 جاءت لتنص على أن إجراء مراقبة الاتصالات الإلكترونية يتخذ للبحث عن الدليل المتعلق بالجريمة، فقد أطلق العنان لاستخدام هذا الإجراء في إطار ممارسة النيابة العامة لعملها في البحث والتحري عن الجرائم، واشترط للقيام بهذا الإجراء:

- أن تتوافر أدلة جديدة.
- وأن يصدر الإذن من قاضي الصلح موجهاً للنيابة العامة لكي تقوم بهذا الإجراء.
- وقد حدده المشرع الفلسطيني بمدة 15 يوماً قابلة للتجديد مرة واحدة فقط، وتأمر النيابة فوراً تجميع المعلومات وتزويدها بها، سواء كانت بيانات متعلقة بحركة الاتصالات أو معلومات الكترونية، أو بيانات

(1) سكورة، مرجع سابق، ص15.
(2) زبيحة زيدان، مرجع سابق، ص127،ص128.

مرور، أو أية معلومات تراها لازمة لمصلحة التحقيقات، وذلك باستعمال الوسائل الفنية والتقنية اللازمة لذلك، ويمكن الاستعانة بمزودي خدمات الانترنت من أجل ذلك[1].

الفرع الثالث: الضبط المعلوماتي.

يقصد بالضبط في مجال الجريمة المعلوماتية هو العثور على الأدلة المتعلقة بالجريمة التي يباشر التحقيق بشأنها، والضبط أو الحجز هو الغاية من التفتيش ونتيجته المباشرة المستهدفة، لذلك يتعين عند إجرائه أن تتوفر فيه نفس شروط التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط[2].

وقد انقسم الفقه حول مسألة مدى خضوع المعلومات للضبط من عدمه كالآتي:

أولاً: مؤيدو ضبط المعلومات.

يرى أصحاب هذا الرأي بأن المعلومات المخزنة آلياً يمكن أن تخضع للحجز أو الضبط وفقاً للقواعد التقليدية للحجز أو الضبط، حتى ولو كانت مجردة عن الدعامة المادية التي تحويها، مستندين في ذلك إلى أن الغاية من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة، وبالتالي يمتد هذا المفهوم التقليدي ليشمل المعلومات بمختلف أشكالها[3].

ثانياً: معارضو ضبط المعلومات.

يرى أصحاب هذا الرأي أنه لا يمكن تصور خضوع المكونات المنطقية للنظم المعلوماتية للحجز، لا سيما إذا ما اتخذت تلك الاجراءات وفقاً للقواعد التقليدية، كون أن المعلومات لا تتمتع بالطابع المادي في حال ما تجردت عن الدعامة المادية التي تحويها[4].

ويتضح لنا موقف كلا المشرعين الجزائري والفلسطيني حول هذه المسألة بمساندة الرأي المؤيد لخضوع المعلومات للحجز أو الضبط، ويتبين ذلك من كونهما أجازوا الحجز أو ضبط المعلومات وفقاً للقواعد التقليدية للحجز أو الضبط، بحيث عندما يتوصل المحققون بعد تفتيش منظومة معلوماتية إلى معلومات من شانها الكشف عن الحقيقة والتوصل لمرتكبي الجرائم المعلوماتية فإنه يجوز ضبطها والتحفظ عليها، وهذا ما جاء في المواد 6، 7 من القانون رقم 09-04 المتعلق بالوقاية من جرائم الإعلام

(1) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، مصدر سابق، المادة 35.
(2) مصطفى محمد موسى، مرجع سابق، ص208.
(3) قريم سكورة، مرجع سابق، ص 74.
(4) سكورة، مرجع نفسه، ص74.

والاتصال الجزائري، والمادتين 34، 38 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني.

وعرّفت المنظمة العالمية لدليل لكمبيوتر الدليل الرقمي بأنه: المعلومات ذات القيمة المحملة والمخزنة أو المنقولة في صورة رقمية.

وتنقسم الأدلة ذات الصلة بالدليل الرقمي إلى 3 أقسام:

1. الدليل الرقمي الأصلي: هو الدلائل المادية والأشياء المحتوية على بيانات متعلقة بالأشياء عند الضبط.
2. الدليل الرقمي المزدوج: هو نتاج إلكتروني دقيق لكل الأشياء الحاملة للمعلومات والموجودة بشكل مادي أصلي.
3. النسخة: هي ناتج دقيق من المعلومات الموجودة في الدليل المادي الأصلي بصرف النظر عن الدلائل المادية الأصلية[1].

ويتم التوصل للدليل المعلوماتي بعدة طرق سنتطرق لأهمها:

1. برنامج إذن التفتيش Computer Scorch Warrant Program .

وهو برنامج قاعدة البيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها، ويمكن لهذا البرنامج أن يصدر ايصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل[2].

2. طريقة النسخ Lap Link.

يتم نسخ المعلومات باستخدام برامج مخصصة لهذا الغرض كبرنامج Lap Link، حيث تؤخذ نسخة من تلك البيانات ثم يتم لصقها وخزنها باسم معين (Sareas) على إحدى منظومات التخزين للمعلومات كالأقراص الصلبة الخاصة بالجهة القائمة بالحجز، ويتم الأخذ بهذه الطريقة من أجل إحراز المعلومات المشفرة بهدف فك شفرتها، كما يتم اللجوء لهذه الطريقة خوفاً من أن يكون النظام المعلوماتي مبرمجاً بالقنبلة الإلكترونية الزمنية التي تؤدي إلى تفجير النظام ذاتياً[3].

---

(1) مصطفى محمد موسى، مرجع سابق، ص215.
(2) مرجع نفسه، ص219.
(3) قريم سكورة، مرجع سابق، ص80.

3. برامج الاتصالات LAN tastic.

وهو جهاز يستطيع من خلاله المحقق وصل حاسوبه بالحاسب الخاص بالمتهم، ويمكنه من نقل ما به من معلومات، ثم حفظها في جهاز لنسخ المعلومات ثم تثبيتها على القرص الصلب، وتعد هذه الطريقة من أهم الطرق التي يتم من خلالها جمع الأدلة الرقمية أو المعلوماتية، والتي يجب أن يقوم بها خبراء في المجال المعلوماتي بالنظر للطبيعة العلمية والدقيقة لهذه الأدلة[1].

هذا بالإضافة إلى طرق أخرى يمكن اللجوء إليها من طرف المحققين لكي يتوصلوا إلى الحقيقة وكشف مرتكبي الجرائم المعلوماتية كبرنامج X tree Pro Gold, AMA Disk, View Disk.

وتتم عملية الضبط وفقاً للقواعد المقررة في كلا التشريعين الجزائري والفلسطيني فيما يتعلق بكيفيات الضبط والتحريز، والحفاظ على سرية المضبوطات من طرف الشرطة القضائية، والاطلاع عليها مخول فقط للجهات التي يحددها القانون، وذلك حفاظاً على مبدأ السرية وحقوق الدفاع.

الفرع الثاني: أعمال التحقيق الخاصة بالقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني.

اشتمل القرار بقانون سابق الذكر على إجراءات أخرى لم ينص عليها المشرع الجزائري في القانون رقم 09-04 المتعلق بالوقاية من جرائم الإعلام والاتصال، وتتمثل في إجراءين وهما: اعتراض الاتصالات، وحجب المواقع الإلكترونية.

أولاً: اعتراض الاتصالات.

وقد تم النص على هذا الإجراء في المادة 37 من القرار بقانون سالف الذكر، بحيث جاءت المادة تشتمل على الآتي:

– يطلب النائب العام أو أحد مساعديه اعتراض محتوى الاتصالات، ثم يصدر إذن من المحكمة المختصة مفاده اعتراض محتوى الاتصالات ، والقيام بتسجيلها أو نسخها، ويتضمن هذا الإذن جميع العناصر التي من شأنها التعريف بالاتصالات محل الاعتراض والأفعال الموجبة له، بالإضافة إلى مدة الاعتراض.

(1) مصطفى محمد موسى، مرجع سابق، ص 220.

– حددت مدة اعتراض محتوى الاتصالات ب 3 أشهر قابلة للتجديد مرة واحدة، ويبدأ حساب هذه المدة من التاريخ الفعلي للقيام بعملية الاعتراض.

– تقوم الجهة المكلفة بتنفيذ الإذن باعتراض الاتصالات بإبلاغ النيابة العامة بالتاريخ الفعلي لانطلاق عملية اعتراض الاتصالات، والتنسيق معها بخصوص اتخاذ جميع الترتيبات التقنية اللازمة لحسن سير عملية الاعتراض[1].

وفي هذا الصدد ومن أجل إتمام العملية بالشكل السليم يجب أن يكون هناك مختصين للقيام لمثل هذه العملية، بحيث أن الصعوبة التي قد تعترض جهات التحقيق للقيام بهذه العملية، فالمشرع منح النيابة العامة إمكانية ندب الخبراء طبقاً لما جاء في قانون الإجراءات الجزائية الفلسطيني رقم 03 لسنة 2001، لا سيما المادة 64 وما يليها منه، فيتم ندب الخبراء المتخصصين في مجال المعلوماتية، بعد استيفاء الشروط المفروضة على الخبير كحلف اليمين، ثم بعد القيام بالعملية يقوم الخبير بتقديم تقرير الخبرة الفنية إلى النيابة العامة، وتخضع الخبرة بشكل كامل لما هو منصوص عليه في قانون الإجراءات الجزائية الفلسطيني[2].

ثانياً: حجب المواقع الإلكترونية.

لقد نصّ المشرع الفلسطيني من خلال القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، لا سيما المادة 40 منه على هذا الإجراء والمتمثل في حجب وإغلاق المواقع الإلكترونية ولكن يتوقف هذا الإجراء على عدة شروط قبل اتخاذه من قبل جهات البحث والتحري، وتتمثل في الآتي:

– رصد مواقع الكترونية مستضافة داخل الدولة أو خارجها.

– تقوم تلك المواقع بوضع عبارات أو أرقام أو صور أو أفلام أو أية مواد دعائية أو غيرها، وكانت تلك المواد تمس وتهدد الامن القومي، أو السلم الأهلي أو النظام العام أو الآداب العامة.

– تقوم جهات البحث والتحري بتقديم محضراً للنيابة العامة وتطلب الإذن بحجب تلك المواقع الالكترونية أو حجب بعض روابطها.

– تقوم النيابة العامة أو أحد مساعديها بطلب الإذن من محكمة الصلح خلال 24 ساعة، ويكون ذلك الطلب مشفوعاً بمذكرة تستعرض رأي النيابة.

---

(1) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، مصدر سابق، المادة 37.

(2) دولة فلسطين، قانون الإجراءات الجزائية رقم 03 لسنة 2001، مصدر سابق، المادة 64 وما يليها.

- تقوم المحكمة بالبت في الطلب في ذات اليوم الذي يعرض عليها فيه أما بقبوله او برفضه[1].

وإجراء حجب المواقع الالكترونية نلاحظ بأن المشرع الجزائري قد نصّ عليه ولكن بطريقة أخرى، بحيث نصّ من خلال المادة 7 من القانون رقم 09-04 المتعلق بالوقاية من جرائم الإعلام والاتصال، على إجراء الحجز عن طريق منع الوصول إلى المعطيات[2].

فهذا الإجراء حدد المشرع الجزائري الظرف التي تتخذ فيه، وهو حالة استحالة الحجز على المعطيات بعد إجراء التفتيش، فإنه يمكن للسلطة المختصة أن تقوم بمنع الوصول إلى تلك المعطيات التي تحتويها المنظومة المعلوماتية والتي قد يكون منها من وجهة نظرنا حجب المواقع الإلكترونية ذات المحتوى الذي من شأنه المساس بالنظام العام والعناصر المكونة له.

المطلب الثاني: إنشاء هيئات متخصصة والتعاون الدولي.

في إطار المكافحة الإجرائية للجريمة المعلوماتية والوقاية من تلك الجرائم، اعتمد كلا المشرعين الجزائري والفلسطيني على إنشاء هيئات ووحدات شرطية متخصصة في المجال المعلوماتي، وذلك للوقاية من وقوع جرائم معلوماتية أو الوصول إلى مرتكبيها بعد وقوعها، وفي هذا الصدد نستعرض الهيئات والأجهزة التي جاء بها كلا التشريعين.

الفرع الأول: الهيئات المتخصصة في التشريع الجزائري.

أولاً: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

تعرف هذه الهيئة بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة وتتولى المهام المنصوص عليها في المادة 14 من القانون رقم 09-04، وذلك تحت رقابة السلطة القضائية وطبقاً لأحكام قانون الإجراءات الجزائية.

تقوم هذه الهيئة المختصة بالجرائم الالكترونية باتخاذ مجموعة من الإجراءات بموجب مقتضيات معينة تتمثل أساساً في حماية النظام العام أو لاستكمال ما يلزم التحريات أو التحقيقات القضائية الجارية

(1) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، مصدر سابق، المادة 40.
(2) الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 16 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مصدر سابق، المادة 7.

وذلك بموجب طلب من السلطة القضائية المختصة من اجل وضع الترتيبات التقنية اللازمة للقيام بالعملية المطلوب القيام بها من طرف الهيئة[1].

1. المهام الموكلة للهيئة.

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- مساعدة السلطات القضائية وأجهزة الشرطة في مجال مكافحة الجرائم المتصلة بالتكنولوجيا من خلال جمع المعلومات وتزويدها بها من خلال الخبرات القضائية.
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الاجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها[2].

2. البناء القانوني للهيئة.

وفقاً للمرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإن البناء القانوني لهذه الهيئة يتشكل من هيئات ادارية وأخرى تقنية وسنتطرق للهيئات التقنية على النحو الآتي:

---

(1) آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة الملتقى الوطني الدولي حول" الإجرام السيبراني المفاهيم والتحديات، جامعة 8 ماي 1945 قالمة، المنعقد يومي 11-12 افريل 2017، ص4.

(2) الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15-261 المؤرخ في 8 اكتوبر2015، الجريدة الرسمية العدد 53، الجزائر، 2015، ص16، المادة 4.

أ. مديرية المراقبة الوقائية واليقظة الإلكترونية.

لم يشر المرسوم الرئاسي رقم 15-261 لتشكيلة هذه المديرية، غير أنه يمكن تحديد تشكيلتها من خلال المادة 18 منه، بحيث تتشكل من مجموعة من ضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية للاستعلام والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، بمساعدة مستخدمي الدعم التقني والإداري من نفس الأسلاك.

وتقوم هذه المديرية بعدد من المهام والتي نذكر منها:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية والقيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية، في الجرائم المنصوص عليها في المرسوم الرئاسي وتحت رقابة القاضي المختص.
- إرسال المعلومات المتحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.
- تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات التي تسمح بتحديد مكان وتواجد مرتكبي الجرائم المعلوماتية والتعرف عليهم، وغيرها من المهام الموكلة إلى هذه المديرية، ومن ذلك نرى بأنها تشكل القطاع العملياتي في هذه الهيئة، بحيث تقوم بجميع العمليات التقنية التي تقوم بها الهيئة في مجال البحث والتحري عن الجرائم المعلوماتية[1].

ب. مديرية التنسيق التقني.

لم ينص المرسوم الرئاسي سالف الذكر على تشكيلة هذه المديرية، إلا أنه يتم تعيين مدير المديرية بموجب مرسوم رئاسي صادر عن رئيس الجمهورية، وتتولى هذه المديرية المهام التالية:

- انجاز الخبرات القضائية في مجال اختصاص الهيئة .
- تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها.
- إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام بمبادرة منها أو بناء على طلب اللجنة المديرة بكل دراسة أو تحليل أو تقييم يتعلق بصلاحياتها مع ضمان تسيير منظومة الإعلام للهيئة وإدارتها[2].

---

[1] مخلوف عكاشة، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور مولاي الطاهر سعيدة، الجزائر، السنة الجامعية 2016-2017،ص67،ص68.

[2] آمال بن صويلح، مرجع سابق، ص7.

ثانياً: الأجهزة الأمنية.

سنتناول دور بعض الأجهزة الأمنية والمراكز البحثية التابعة لها في التصدي للجريمة المعلوماتية على النحو الآتي:

1. المديرية العامة للأمن الوطني.

تتصدى هذه المديرية للجريمة المعلوماتية من عدة جوانب وأهمها الجانب التوعوي، بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية والتوعية، وهذا من خلال برمجتها لتنظيم دروس في مختلف الأطوار الدراسية، وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شانها توعية المواطن حول خطورة الجرائم الالكترونية.

وفي إطار مكافحة الجريمة المعلوماتية ونظراً للبعد الدولي الذي عادة ما يتخذه ها النوع من الجرائم، فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية (الإنتربول)، هذه الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الإنابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دولياً[1].

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام.

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام، أحد أهم المؤسسات المتخصصة في مكافحة الإجرام المعلوماتي، تم إنشاؤه بمرسوم رئاسي رقم 04-183 سنة2004، وذلك في إطار عصرنة قطاع الدرك الوطني الجزائري، وهو أداة مستوحاة من الخبرات العملية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة، ويتشكل المعهد من عدة دوائر والتي منها " **دائرة الإعلام الآلي والإلكترونيك**"، والتي تختص بتحليل الأدلة الجنائية الخاصة بالجريمة المعلوماتية، وتقوم بتحليل وإصلاح الدعامات الإلكترونية التي يتم التحصل عليها بعد عمليات التفتيش أو المعاينة، كما تقوم بالمقاربات الهاتفية، وتحسين جودة التسجيلات الصوتية والفيديو إذا ما كانت جودتها رديئة[2].

(1) عاقلي فضيلة، مرجع سابق، ص133.
(2) مخلوفي عكاشة، مرجع سابق، ص77.

ويقوم هذا المعهد بعدد من المهام في إطار البحث والتحري عن الجرائم المعلوماتية كالآتي:

- القيام بالخبرات العلمية أو الخبرات اللازمة في توجيه التحقيقات القضائية، من أجل الكشف عن الحقيقة ومرتكبي الجرائم المعلوماتية.
- مساعدة المحققين للسير الحسن للمعاينات، من خلال دعمهم بالفنيين المؤهلين عند الحاجة.
- تنفيذ مناهج الشرطة العلمية والتقنية المتعلقة بجمع وتحليل الأدلة المعلوماتية.
- ضمان المساعدة العلمية في الحريات المعقدة كالوضع في الحريات الخاصة بالجريمة المعلوماتية.
- المشاركة في الأبحاث والتحاليل المتعلقة أساساً بتقليل جميع أشكال الإجرام المعلوماتي.
- مشاركة ومساهمة المعهد بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام[1].

الفرع الثاني: الهيئات المتخصصة في التشريع الفلسطيني.

لقد نصت المادة 1/03 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية على ما يلي: " **1- تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوى الأمن على أن تتمتع بصفة الضابطة القضائية، وتتولى النيابة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه** ".

وفي إطار مكافحة الجريمة المعلوماتية فقد استحدثت عدة أجهزة للتصدي لهذا النوع من الجرائم والتي سنتعرض لها على النحو الآتي:

أولاً: استحداث نيابة عامة متخصصة في الجرائم الإلكترونية.

تعتبر النيابة العامة احد العناصر الأساسية في أي نظام قضائي، والتي تعبر عن حق المجتمع في المحافظة على أمنه واستقراره، فعمل النيابة يتمثل أساساً في البحث والتحري عن الجرائم والتوصل لمرتكبي الجرائم، وتقوم بذلك وفق الخطط التي تضعها والاستراتيجيات التي تراها مناسبة للعمل القضائي من أجل إحكام القبضة على مجرمي المعلوماتية، وكذا فرض القانون على المجتمع.

وفي إطار مكافحة الجريمة المعلوماتية تم إنشاء نيابة متخصصة بالجرائم الإلكترونية وذلك بقرار من النائب العام وذلك بتاريخ 2016/3/20، وذلك بعد الانتشار الواسع للجريمة المعلوماتية في المجتمع

[1] مخلوفي عكاشة، مرجع سابق، ص78.

الفلسطيني، وتتشكل هذه النيابة من 26عضوتً مختصين تقنياً وفنياً في التحقيق بالجرائم المعلوماتية، ومن بينهم وكلاء ومعاونين نيابة في كل محافظات الوطن، ويشرف عليها النائب العام[1].

وتعمل أساساً هذه النيابة وبالنظر لاختصاصها في مجال الجرائم المعلوماتية، بالبحث والتحري عن جميع الجرائم التي تصنف كجريمة معلوماتية، ونظراً لحداثة هذه الجريمة وارتكابها في الفضاء السيبراني يستدعي أن يكون المحققين فيها على دراية واسعة بمجال المعلوماتية، وذلك لتخطي أي عائق قد يواجه المحققين أثناء قيامهم بعمليات التفتيش الالكتروني وكذا ضبط المعطيات التي تحويها الأنظمة المعلوماتية.

وتعتبر هذه النيابة المتخصصة نقلة نوعية في مجال التحقيق المعلوماتي، خاصةً وأن المنظومة القانونية الفلسطينية كانت تعاني من الفراغ التشريعي في التصدي للجريمة المعلوماتية من الناحية التجريمية، وبعد صدور القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، أصبحت هناك شرعية تجريمية، الأمر الذي يسمح للنيابة العامة تسهيل عملها من حيث إعطاء التكييف القانوني المناسب للجرائم المعلوماتية المرتكبة، وكذا منح النيابة العامة شرعية إجرائية فيما يتعلق بتفتيش النظم المعلوماتية، وعمليات الضبط والحجز على المعلومات، والذي ثار حولهما جدلاً فقهياً كما أسلفنا سابقاً.

ثانياً: وحدة الجرائم الإلكترونية على مستوى جهاز المباحث العامة.

تتولى المباحث العامة مهام البحث والتحري وملاحقة وكشف الجرائم ومرتكبيها، وفي سبيل الكشف عن الجرائم أصبحت تعتمد على الوسائل العلمية الحديثة وتوظيفها في عملها، ويقوم هذا الجهاز بتطوير المهارات والمعارف اللازمة للقيام بمهامها على أكمل وجه[2].

بحيث تم إنشاء وحدة متخصصة ضمن جهاز المباحث العامة الفلسطينية يختص بالبحث عن الجرائم الإلكترونية، وتقوم هذه الوحدة أساساً بالبحث والتحري عن الجرائم المعلوماتية، وذلك لما يتمتع به أعضائها من خبرة فنية وتقنية في المجال المعلوماتي، بالإضافة إلى القيام بإجراءات المراقبة الإلكترونية للاتصالات وإجراءات التفتيش الإلكتروني بعد تلقيها الإذن من النيابة العامة كونها تتمتع بصفة الضبط القضائي.

---

(1) نبيل محمود فريد أبو الرب، مرجع سابق، ص67.

(2) موقع الكتروني، http://www.palpolice.ps/ar، تاريخ الاطلاع 2018/3/17.

الفرع الثالث: التعاون الدولي.

بـالرجوع إلـى أحكـام القـانون رقـم 09-04 الجزائـري، والقـرار بقـانون رقـم 16 لسـنة 2017 الفلسطيني، نجد بأن كلا القانونين قد نصّا على التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، كونها جريمة عابرة للحدود الوطنية، ومن ذلك نستعرض أحكام المساعدة القضائية الدولية.

أولاً: مجالات التعاون الدولي.

أ- المساعدة القضائية الأمنية.

مفاد هذا التعاون أن الدولة وحدها لا تستطيع مجابهة التطور العلمي والتكنولوجي الحاصل، لا سيما في مجال الجريمة المعلوماتية، خاصة الجرائم التي ترتكب على شبكات الإنترنت، والتي تشكل خطراً ليس فقط على سرية نظم الحاسوب، بل تعدت إلى أمن البنى الأساسية الحرجة، وبالنظر للطابع الدولي للجريمة المعلوماتية، لابدّ من وجود تعاون دولي في إطار مكافحتها بين أجهزة الشرطة في الدول على اختلافها، وذلك من خلال إنشاء مراكز يتمحور عملها بالبحث عن مرتكبي الجرائم المعلوماتية وتعميمها على الأجهزة الشرطية الأخرى.

وفي نفس الصدد هناك من الجرائم التي تمتد أركانها إلى أكثر من دولة، كجرائم البث الفيروسي، فبهذه الحالة تقع الحدود الوطنية عائقاً أمام التحريات عن مرتكب الجريمة، لذلك كان لا بدّ من وجود تعاون دولي بين أجهزة الشرطة المختلفة، من أجل الحد من هذه العوائق التي تعترض المحققين عند القيام بأعمالهم، في مجال البحث والتحري عن الجرائم المعلوماتية[1].

ب-المساعدة القضائية في مجال تسليم المجرمين.

استقر الفقه الدولي، باعتبار تسليم المجرمين أحد أشكال التعاون الدولي في مكافحة الجرائم لا سيما الجرائم المعلوماتية، وإلقاء القبض على المجرمين، ويعتبر هذا التعاون وليد التطورات التي تحدث على مستوى كافة المجالات لا سيما مجال تكنولوجيا المعلومات، وتسليم المجرمين يعمل دون حيلولة الحدود عائقاً أمام مرتكبي الجرائم المعلوماتية، بحيث أن السلوك الإجرامي للمجرم المعلوماتي لا يقتصر على الإقليم الذي يرتكبها فيه، بل يتعدى ذلك ليشمل أقاليم دول أخرى.

[1] إحسان طبال، مرجع سابق، ص324.

وكون أن أجهزة البحث والتحري في الدولة تلتزم بالنطاق الإقليمي المحدد لها، فإنها لا تستطيع ملاحقة مرتكبي الجرائم المعلوماتية الذين يفرّوا إلى الخارج، كان لا بدّ من خلق آلية دولية من أجل التعاون مع الدول الأخرى لملاحقة مرتكبي الجرائم بصفة عامة والجرائم المعلوماتية على وجه الخصوص، ويقوم نظام تسليم المجرمين على أساس أن الدولة التي يفرّ إليها المجرم بارتكابه لأحد الجرائم المعلوماتية، تقوم تلك الدولة بمحاكمة ذلك المجرم وفقاً لتشريعها إذا ما كان يجرّم الفعل الذي اقترفه، فتسليم المجرمين نظام يعمل على تحقيق مصلحة الدولتين، فالدولة الأولى تضمن توقيع العقاب على مرتكب الجريمة، والدولة الثانية المطالبة بتسليم المجرم كونه يعمل على تطهير إقليمها من المجرمين وحتى لا تصبح ملاذاً للمجرمين الفارين من العدالة[1].

ج- التعاون الدولي في مجال التدريب.

من أجل مكافحة الجرائم المعلوماتية والتي تعتمد غالبيتها على تكنولوجيا المعلومات والإنترنت، فإن التعاون الدولي في مجال التدريب، يعمل على تطوير المهارات الفنية والتقنية لجهات البحث والتحري، مما يجعها تسير بخطوات متناسقة مع التطورات السريعة الحاصلة على تكنولوجيا المعلومات، وذلك بهدف الإلمام بها من أجل مكافحة الجريمة المعلوماتية بكافة صورها هذا من جهة، ومن جهة أخرى فإن الإجراءات المتخذة في مواجهة الجريمة المعلوماتية تتجاوز المفاهيم والمبادئ التقليدية المتعارف عليها في التشريع العقابي، نظراً لما تتسم به هذه الجريمة من حداثة في الأسلوب المستخدم في ارتكاب الجريمة وسرعة في تنفيذها وسهولة طمس الدليل فيها[2].

فجهات البحث والتحري عن الجرائم المعلوماتية لا بدّ أن تكون على درجة عالية من المهارة والخبرة الفنية والتقنية في هذا المجال، وقدرتها على كشف الغموض في تلك الجرائم، والوصول إلى مرتكبيها في أسرع وقت، وهذا الأمر لن يتحقق إلا بالتدريب، فكفاءة رجال العدالة في مواجهة الإجرام المعلوماتي تتوقف على قدرتهم والتي لا بد لها أن ترتكز على كيفية تطوير العملية التدريبية والارتقاء بها من أجل تحقيق أهدافها، لذلك كان وجوباً تأهيل القائمين على هذه الأجهزة[3].

(1) إحسان طبال، مرجع سابق، ص326،ص327.
(2) مرجع نفسه، ص327.
(3) مرجع نفسه ،ص328.

ثانياً: القيود الواردة على المساعدة القضائية الدولية في القانون رقم 09-04.

لقد حصرتها المادة 18 من القانون رقم 09-04 فيما يلي:

1. أن المساعدة القضائية الدولية لا تنفذ ولا يتم الاستجابة لها في الحالات الآتية:
- إذا كان فيها مساس بالسيادة الوطنية.
- إذا كانت ماسة بالنظام العام.

2. يمكن الاستجابة للمساعدة القضائية الدولية في الحالات الآتية:
- شرط المحافظة على سرية المعلومات المبلغة لتلك الدولة.
- شرط عدم استعمالها في غير الحالة المحددة والموضحة حصرياً في طلب المساعدة القضائية، وقد ألزمت الاتفاقية الدولية الموضوعة للتوقيع بمقر الأمم المتحدة في نيويورك 2005/09/14، والخاصة بقمع أعمال الإرهاب النووي، بحيث ألزمت الدول الأطراف باتخاذ التدابير لحماية سرية المعلومات التي يحصل عليها سراً بموجب الاتفاقية من دولة أخرى.

ومما لا شك فيه أن السلطات الجزائرية قد لبت العديد من الأعمال الجزائية في إطار المساعدات القضائية الدولية، واتخذت عدة تدابير منها إحالة المتهمين على العدالة، وعلى سبيل المثال: تم فتح تحقيق قضائي في 800 قضية متعلقة بالجريمة الإلكترونية منذ دخول القانون رقم 09-04 حيز التنفيذ، وهي القضايا التي تورط فيها جزائريون وأجانب استهدفت شبكات وقواعد بيانات لمؤسسات جزائرية وأجنبية، ونذكر منها تمت متابعة شاب جزائري وإحالته على العدالة، بحيث قام هذا الشاب باختراق موقع لشركة أمريكية متخصصة في حماية المعلومات والبرامج الإلكترونية للعديد من الشركات الأمريكية، ثم عمل على استغلال المعلومات التي تحصل عليها لصالح شركات منافسة مقابل مبالغ مالية، وعلى إثر ذلك أودعت الشركة المتضررة شكوى لدى الشرطة الأمريكية، وقدمت هذه الاخيرة المعلومات الكافية بشأن المتهم المشار له إلى مصالح الأمن الجزائرية، بحيث تم تقديم المتهم للمحاكمة امام محكمة جنح باتنة[1].

[1] زبيحة زيدان، مرجع سابق، ص146،ص147.

ثالثاً: القيود الواردة على المساعدة القضائية الدولية في القرار بقانون رقم 16 لسنة 2017.

لقد نصّ المشرع الفلسطيني من خلال المادتين 43 و44 من القرار بقانون سالف الذكر، على المساعدة القضائية الدولية، مع الجهات المختصة الأجنبية وذلك في حدود ما يسمح به القانون، بحيث نظم أحكامها على النحو الآتي:

1. تقوم الجهات المختصة بتسهيل التعاون مع الجهات المختصة للدول الأجنبية، ويكون ذلك مبيناً على اتفاقيات دولية وإقليمية وثنائية تمت المصادقة عليها من كلا الدول طالبة المساعدة، أو تتم المساعدة القضائية الدولية طبقاً لمبدأ المعاملة بالمثل.
2. يكون الهدف من تبادل المساعدة القضائية الدولية هو الإسراع في تبادل المعلومات على نحو من شأنه أن يكفل الإنذار المبكر بجرائم ماسة بأنظمة المعلومات والاتصال وتفادي وقوعها، والمساعدة على التحقيق فيها وتتبع مرتكبيها.
3. ولكي تنفذ المساعدة القضائية الدولية يجب على الدولة الأجنبية طالبة المساعدة أن تقوم بالحفاظ على سرية المعلومات المحالة إليها بموجب طلب المساعدة، وتلتزم الدولة بعد إحالتها إلى أي طرف أخر من أجل استغلالها لأغراض أخرى غير مكافحة الجرائم الإلكترونية[1].

كما استكمل المشرع الفلسطيني تنظيم أحكام المساعدة القضائية الدولية من خلال المادة 44 من القرار بقانون سابق الذكر بحيث اشترط ما يلي:

– يتوجب على الجهات المختصة تقديم العون للجهات الأجنبية طالبة المساعدة، وتسليم المجرمين عندما يتعلق الأمر بالجرائم الإلكترونية، وتتخذ وفقاً لما يقرره قانون الإجراءات الجزائية والاتفاقيات الثنائية أو الاتفاقيات متعددة الأطراف شريطة أن تكون الدولة طرفاً فيها، أو تتم المساعدة القضائية طبقاً لما يقتضيه مبدأ المعاملة بالمثل.

– وطلب المساعدة القضائية أو طلب تسليم المجرمين لا ينفذ إلا بشرط أن يكون الفعل موضوع الطلب مجرّماً في تشريع الدولة طالبة المساعدة أو تعاقب على جريمة مماثلة بحيث تعتبر ازدواجية التجريم مستوفاة، حتى ولو كانت الجريمة منصوص عليها بمصطلح مغاير أو يصنف ضمن فئة أخرى من الجرائم، فالشرط ينصّب على أن يكون الفعل موضوع الطلب مجرّماً في تشريع الدولة طالبة المساعدة[2].

---

(1) دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية، مصدر سابق، المادة 43.
(2) دولة فلسطين، مصدر نفسه، المادة44.

خلاصة الفصل:

يعتبر قانون الإجراءات الجزائية المرجعية الأساسية للإجراءات المتخذة بعد ارتكاب الجريمة من بداية اجراءات الاستدلال مروراً بتحريك الدعوى العمومية والتحقيقات المنبثقة عنها وصولاً للنطق بالحكم على المجرم، وتلك الاجراءات احاطها المشرع بضوابط وقيود، فقواعد الاختصاص القضائي تبقى هي المنصوص عليها في قانوني الاجراءات الجزائية الجزائري والفلسطيني سواء كانت قاعدة عامة أو استثناء، اما القانون الواجب التطبيق على الجريمة المعلوماتية فهو مبدأ الإقليمية واستثناءً مبدأ عينية أو شخصية النص الجنائي، وفي حالة ارتكب جزء من الفعل في دولة والجزء الآخر في دولة الجزائر او فلسطين فيطبق عليه قانون العقوبات سواء الجزائري أو الفلسطيني باعتبار أن إرتكاب جزء من الجريمة على أراضيها كمن إرتكب الجريمة كاملة في إقليم الدولة الجزائرية أو الفلسطينية.

وجاء قانون الإجراءات الجزائية الجزائري بإجراءات تحقيق خاصة في مجال الجريمة المعلوماتية كالتسرب وغيره من الإجراءات، كوسيلة لمواجهة هذا النوع من الجرائم، إلا أننا نجد عكس ذلك في قانون الإجراءات الجزائية الفلسطيني بحيث اكتفى بالوسائل التقليدية في الإثبات الجنائي كالخبرة والتفتيش وما إلى ذلك من الإجراءات.

أما القوانين الخاصة التي نصت على إجراءات متعلقة بالجريمة المعلوماتية فنجد القانون رقم 09-04 الجزائري، والقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني، فجاء كل منهما بإجراءات منها ما هو مشترك ومنها ما هو خاص بالقانون الفلسطيني دون القانون الجزائري، من الاجراءات المشتركة هي التفتيش المتعلق بالجريمة المعلوماتية وما يحمله من طابع خاص كونه يتخذ داخل الكمبيوتر وشبكاته، وكذا مراقبة الاتصالات الإلكترونية والتقنيات المستخدمة في عملية المراقبة كبرنامج كارنيفور، وأيضاً الضبط وأنواع الدليل الرقمي المضبوط وتقنيات الضبط، ومن جهة أخرى نجد أن القرار بقانون رقم 16 لسنة 2017 الفلسطيني جاء بإجراءات خاصة كاعتراض الاتصالات وحجب المواقع الالكترونية.

ومما جاء في القوانين الخاصة هي الهيئات المتخصصة التي وردت في القانونين 09-04 الجزائري والقرار بقانون رقم 16 لسنة 2017 الفلسطيني، وعلى سبيل المثال: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته الجزائرية، وكذا إنشاء أجهزة شرطية خاصة بالجريمة المعلوماتية تتبع الشرطة الفلسطينية، وتحديد كيفيات وشروط المساعدة القضائية الدولية لمكافحة الاجرام المعلوماتي وتبادل المعارف والخبرات.

الخاتمة

لقد تناولنا بالدراسة مكافحة الجريمة المعلوماتية من ناحيتين، الناحية الموضوعية وهي شق التجريم والعقاب على الجريمة المعلوماتية سواء في قانون العقوبات أو من خلال القوانين الخاصة المكملة لقانون العقوبات أو تلك المتعلقة بالملكية الفكرية، والناحية الإجرائية تطرقنا لقواعد الاختصاص المتعلقة بالجريمة المعلوماتية من حيث المحاكم والنيابة العامة وكذا الشرطة القضائية وأعمال التحقيق في الجريمة المعلوماتية والجهات القائمة عليها، بالإضافة إلى الإجراءات الخاصة التي وردت في القوانين الخاصة والهيئات المتخصصة المناط بها البحث والتحري عن الجريمة المعلوماتية التابعة لكلا الدولتين الجزائرية والفلسطينية.

نرى بأن كلا المشرعين الجزائري والفلسطيني على حد السواء، قد مروا بفترة كان بها التشريع العقابي غير قادر على التصدي للجرائم المعلوماتية، نظراً لانعدام النصوص الجنائية التي تعاقب على هذا النوع من الجرائم، وكونها جريمة غير كلاسيكية وترتكب في الفضاء السيبراني وتعتمد في إرتكابها على وسائل تكنولوجيا المعلومات الحديثة، الأمر الذي جعل القضاء في كلا الدولتين يتجه إلى تطويع النصوص الجنائية التقليدية على الجريمة المعلوماتية، ولكن تطبيق النصوص المتعلقة بجرائم الأموال على الجريمة المعلوماتية يصطدم بمبدأ الشرعية الجنائية.

ثم اتجه بعد ذلك المشرع الجزائري إلى خلق نصوص جنائية متعلقة بالتجريم والعقاب على الجريمة المعلوماتية في القسم السابع مكرر من قانون العقوبات تحت عنوان الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد استعمل المشرع مصطلحات مرنة نوعاً ما لكي يتفادى التعديلات المستمرة للنصوص في كل مرة ترتكب فيها جريمة جديدة، إلا أن المشرع الفلسطيني على النقيض من نظيره الجزائري فلم يستحدث أي نصوص تذكر من خلال قانون العقوبات سواء المطبق في الضفة الغربية أو المطبق في قطاع غزة، وفي ظل هذا الفراغ التشريعي المستمر كانت النيابة العامة الفلسطينية تعتمد في تأسيس دعواها على نصوص جرائم الأموال.

ومن جهة أخرى فقد جاءت القوانين الخاصة لا سيما القوانين المكملة لقانون العقوبات على تجريم بعض الأفعال التي ترتكب من خلال وسائل تكنولوجيا المعلومات في كلا التشريعين الجزائري والفلسطيني، فعلى سبيل المثال تم تجريم ترويج المخدرات والمؤثرات العقلية من خلال الوسائل الإلكترونية وذلك من

خلال قانون مكافحة المخدرات والمؤثرات العقلية الجزائري والفلسطيني أيضاً، ولعل أهم تلك القوانين الخاصة هو القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الذي جاء ليجرّم الأفعال التي تشكل جريمة معلوماتية في فلسطين.

وفي نفس الصدد تناولنا أهمية القوانين المتعلقة بالملكية الفكرية في فرض الحماية الجنائية على المعلوماتية، بحيث نجد بأن القوانين المتعلقة بالملكية الصناعية يصعب حماية برامج الكمبيوتر من خلالها نظراً لصعوبة تحقيق الشروط الخاصة بمنح براءة الاختراع وذلك في كلا التشريعين، أما القوانين المتعلقة بالملكية الفكرية وحق المؤلف فيمكن حماية برامج الكمبيوتر من خلالها باعتبارها أحد المصنفات الفنية وهذا بالإستناد للقوانين المطبقة في الجزائر وفلسطين.

ومن جهة أخرى فإن قواعد الاختصاص الاقليمي للمحاكم وجهات النيابة العامة وكذا الشرطة القضائية تخضع لما هو مقرر في قانون الإجراءات الجزائية الجزائري وكذا الفلسطيني، وفيما يتعلق بأعمال التحقيق فقد جاء قانون الإجراءات الجزائية الجزائري بإجراءات خاصة فيما يتعلق بالجريمة المعلوماتية والتحقيق فيها، أما قانون الإجراءات الجزائية الفلسطيني فلم يشتمل على إجراءات خاصة بالجريمة المعلوماتية وأحاطها بالإجراءات التقليدية المتعارف عليها.

وفي سياق متصل جاءت القوانين الخاصة لا سيما القانون 09-04 الجزائري بإجراءات خاصة تتخذ في مواجهة الجريمة المعلوماتية، وكذا القرار بقانون رقم 16 لسنة 2017 سالف الذكر جاء بإجراءات خاصة من أجل التصدي لهذه الجريمة، ومن هذه الإجراءات ما هو مشترك بين التشريعين، ومنها ما هو مختلف أو جاء ذكره بصياغة أخرى، وتعرّض كلا القانونيْن للمساعدة القضائية الدولية في مجال الجريمة المعلوماتية.

ومما سبق ذكره نستنتج ما يلي:

1. تطويع النصوص الجنائية التقليدية على الجريمة المعلوماتية، لا يمكن إعماله بشأن الجرائم التي تعتمد على التكنولوجيا أو ترتكب بواسطة الإنترنت كونها تخرج عن الطبيعة المادية التي تشترطها جرائم الأموال حتى ولو اعتبرناها من قبيل الأموال المعنوية فإن بعض الأفعال لا يمكن تطويع تلك النصوص بشأنها كفعل الدخول إلى النظام المعلوماتي.

2. وُفّقَ المشرع الجزائري عند استحداثه للقسم السابع مكرر من قانون العقوبات المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات كونه استخدم مصطلحات قانونية مرنة تمكّن من تجريم الأفعال التي يمكن أن تستحدث مستقبلاً، خلافاً لما هو معمول به في بعض الدول التي تقوم بتقنين كل جريمة على حدى.

3. واستكمالاً للنقطة السابقة، يهدف المشرع الجزائري إلى الوقاية من إرتكاب الجريمة المعلوماتية، بحيث لا ينتظر وقوع الجريمة وإفلات مرتكبها من العقاب إلى حين تقنين الفعل بموجب نص خاص به حتى يتم معاقبته، فتدارك ذلك باستخدام مصطلحات مرنة.

4. تختلف الحماية الجنائية بين المشرعين الجزائري والفلسطيني بحيث أن قانون العقوبات الجزائري اشتمل على نصوص خاصة بالجريمة المعلوماتية على العكس من نظيره الفلسطيني الذي خلا من أي نص يتعلق بالجريمة المعلوماتية في قانون العقوبات.

5. ويكمن الإختلاف أيضاً في أن المشرع الفلسطيني أصدر قانوناً خاصاُ يتعلق بالجرائم المعلوماتية على العكس من المشرع الجزائري الذي اكتفى بالنصوص التي وردت في قانون العقوبات.

6. ويتضح الإختلاف أيضاً من خلال الإجراءات الخاصة لمواجهة الجريمة المعلوماتية التي أوردها المشرع الجزائري في قانون الاجراءات الجزائية لا سيما إجراء التسرب وإلتقاط الصور، فهذين الإجراءين لم ينص عليهما المشرع الفلسطيني ولا في أي موضع.

7. يشترك كلا المشرعين الجزائري والفلسطيني بالحماية الجنائية من الجريمة المعلوماتية من خلال القوانين المكملة لقانون العقوبات بحيث تناول كلاً منهما صوراً للجريمة المعلوماتية كترويج المخدرات عن طريق الانترنت.

8. يتشابه كلا التشريعين الجزائري والفلسطيني من حيث عدم إمكانية حماية برامج الكمبيوتر من خلال قانون الملكية الصناعية لصعوبة توافر الشروط المطلوبة لمنح براءة الإختراع.

9. ويتشابه كلا التشريعين أيضاً من خلال قوانين الملكية الفكرية بحيث يمكن حماية برامج الكمبيوتر من خلالها باعتبارها مصنفاً فنياً ويمكن أن تقع عليه جريمة التقليد.

10. ويتبين لنا التشابه في كلا التشريعين من خلال الإجراءات المنصوص عليها سواء في قانون الاجراءات الجزائية أو القوانين الإجرائية الخاصة كالتفتيش والضبط والتعاون الدولي وغيرها من الإجراءات التي تتخذ في مواجهة الجريمة المعلوماتية، فهي إجراءات مشتركة بين التشريعين، ولكن ما جاء من اجراءات في قانون الاجراءات الجزائية الجزائري أورده المشرع الفلسطيني في القرار بقانون بشان الجرائم الإلكترونية.

11. أدى الفراغ التشريعي قبل صدور القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية إلى شل يد العدالة الفلسطينية وإفقادها الشرعية الجنائية بشقيها التجريمي والإجرائي.

12. جاء القرار بقانون رقم 16 لسنة 2017 بشان الجرائم الإلكترونية والذي جرّم العديد من الأفعال، واستخدامه لمصطلحات فضفاضة بشكل كبير، الأمر الذي جعل منه محل إنتقاد من طرف المؤسسات الحقوقية الفلسطينية.

13. تناقض القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية من حيث النظام العقابي، بحيث اشتمل على عقوبات جنحوية إلى جانب العقوبات الجنائية وهو ما يخالف النظام العقابي المنصوص عليه في قانون العقوبات لا سيما المطبق في الضفة الغربية.

14. نجاعة الإجراءات الخاصة التي جاء بها قانون الإجراءات الجزائية الجزائري في إطار محاربة الجريمة المعلوماتية، وذلك تماشياً مع الطبيعة الخاصة للجريمة المعلوماتية لا سيما وأنها سريعة الارتكاب وسهولة طمس الأدلة فيها.

15. افتقار قانون الإجراءات الجزائية رقم 03 لسنة 2001 الفلسطيني لأي إجراءات خاصة تتعلق بالبحث والتحري عن الجرائم المعلوماتية، الأمر الذي تداركه من خلال القرار بقانون رقم 16 لسنة 2017 بنصّه على إجراءات خاصة بتتبع مرتكبي الجرائم المعلوماتية ، وهي إجراءات ذات فاعلية في إطار مكافحة الإجرام المعلوماتي.

ومما سبق استنتاجه نقترح التوصيات الآتية:

1. ضرورة البحث في مجال الجريمة المعلوماتية خاصة الدارسين للقانون في فلسطين، وذلك لنقص الدراسات المتخصصة في هذا المجال.
2. ضرورة تعديل القرار بقانون رقم 16 لسنة2017 لإزالة التناقض في النظام العقابي، فالجمع بين عقوبتين جنائية وجنحية في نفس النص، يؤدي بالقضاة إلى الحياد عن تطبيق العدالة.
3. وفي نفس السياق ضرورة مراجعة القرار بقانون رقم 16 لسنة 2017، بحيث يشتمل على مصطلحات يشوبها الغموض، فعلى المشرع إعطائها الوصف الدقيق، كونها مصطلحات فضفاضة بشكل كبير، الأمر الذي يفتح الباب واسعاً أمام القضاة للتأويل والقياس فيها.
4. نشر الوعي القانوني في أوساط المجتمع حول مخاطر الجريمة المعلوماتية، وضرورة الإبلاغ عنها للجهات المختصة في كلا الدولتين الجزائرية والفلسطينية.
5. تكثيف التدريبات من أجل تنمية وتطوير واكتساب المهارات الفنية والتقنية في المجال المعلوماتي من طرف المحققين المختصين بهذا النوع من الجرائم، من أجل الحد من انتشار ظاهرة الإجرام المعلوماتي، ويستوي الأمر بين الدولتين كذلك.
6. ضرورة التعاون بين الدولتين الجزائرية و الفلسطينية في مجال التعاون الدولي في مكافحة ظاهرة الإجرام السيبراني وذلك للحد من هذه الجريمة .

قرار بقانون رقم (16) لسنة 2017م
بشأن الجرائم الإلكترونية

رئيس دولة فلسطين
رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

استنادا لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على قانون رقم (74) لسنة 1963م وتعديلاته، الساري في المحافظات الجنوبية، وعلى أحكام قانون العقوبات الأردني رقم (16) لسنة 1960م وتعديلاته، الساري في المحافظات الشمالية،
وعلى قانون رقم (3) لسنة 1996م، بشأن الاتصالات السلكية واللاسلكية،
وعلى قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته،
وعلى القرار بقانون رقم (18) لسنة 2015م، بشأن مكافحة المخدرات والمؤثرات العقلية،
وعلى قرار بقانون رقم (20) لسنة 2015م، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته،
وبناءً على تنسيب مجلس الوزراء بتاريخ 20/06/2017م،
وعلى الصلاحيات المخولة لنا،
وتحقيقا للمصلحة العامة،
وباسم الشعب العربي الفلسطيني،

أصدرنا القرار بقانون الآتي

مادة (1)
يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك:
الوزارة: وزارة الاتصالات وتكنولوجيا المعلومات.
الوزير: وزير الاتصالات وتكنولوجيا المعلومات.
معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات، أو استلامها، أو تسجيلها، أو تخزينها، أو تعديلها، أو نقلها، أو استرجاعها، أو محوها، أو نشرها، أو إعادة نشر بيانات، أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤه أو تعديل محتوياته.
تكنولوجيا المعلومات: هي أية وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أية وسيلة أخرى سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات، أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة.
البيانات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها.
المعلومات الإلكترونية: أية معلومة يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تكنولوجيا المعلومات بوجه خاص بالكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها.
الشبكة الإلكترونية: هي ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت).
السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفا لحالة تتعلق بشخص أو شيء ما؛ والتي يتم إنشاؤها، أو إرسالها، أو تسلمها، أو تخزينها بوسائل إلكترونية.
المستند الإلكتروني: هو السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينها أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.
الموقع الإلكتروني: هو مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد.

الشخص: الشخص الطبيعي أو المعنوي.
التطبيق الإلكتروني: هو برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر؛ يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها.
بيانات المرور: أية بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته ونوع خدمة الاتصال.
كلمة السر: هي كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات وما في حكمها للتأكد من هويته وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها.
وسيلة التعامل الإلكتروني: هي البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك.
البيانات الحكومية: يشمل ذلك بيانات الدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها.
التشفير: هو تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية.
الشفرة: هي مفتاح، أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز أو ما في حكمها.
الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها.
الاختراق: هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.
التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره بغرض الموافقة على مضمون المعاملة.
أداة التوقيع: هي برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.
الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني.
مزود الخدمة: هو أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أية خدمة إلكترونية أو مستخدمي هذه الخدمة.
الإتلاف: هو تدمير البرامج الإلكترونية سواء أكان كليا أم جزئيا، أو جعلها على نحو غير صالحة للاستعمال.
معلومات المشترك: أية معلومة موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات بما في ذلك:

- نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
- هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة.
- أية معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.

الموظف: كل من يعمل في القطاع العام، أو الخاص، أو المؤسسات الخاصة، أو الهيئات المحلية والأهلية، أو الجمعيات، أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم.

مادة (2)

1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء أكان الفاعل أصلياً، أم شريكاً، أم محرضاً، أم متدخلاً، على أن تكون الجرائم معاقباً عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.
2. يجوز ملاحقة كل من يرتكب خارج فلسطين إحدى الجرائم المنصوص عليها بهذا القرار بقانون في إحدى الحالات الآتية:

أ. إذا ارتكبت من مواطن فلسطيني.
ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية.
ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية.

مادة (3)

1. تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطية وقوى الأمن على أن تتمتع بصفة الضابطة القضائية، وتتولى النيابة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه.
2. تتولى المحاكم النظامية والنيابة العامة، وفقاً لاختصاصاتهما، بالنظر في دعاوى الجرائم الإلكترونية.

مادة (4)

1. كل من دخل عمداً وبدون وجه حق بأية وسيلة موقعاً إلكترونياً، أو نظاماً، أو شبكة إلكترونية، أو وسيلة تكنولوجيا معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.
2. إذا ارتكب الفعل المحدد في الفقرة (1) من هذه المادة على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة شهور أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما.
3. إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي، أو حذفها، أو إضافتها، أو إفشاؤها، أو إتلافها، أو تدميرها، أو تغييرها، أو نقلها، أو التقاطها، أو نسخها، أو نشرها، أو إعادة نشرها، أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني، أو إلغاؤه، أو تعديل محتوياته، أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
4. إذا ارتكب الفعل المحدد في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (5)

كل من أعاق أو عطل الوصول إلى الخدمة، أو الدخول إلى الأجهزة، أو البرامج أو مصادر البيانات، أو المعلومات، بأية وسيلة كانت عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو بالعقوبتين كلتيهما.

مادة (6)

كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل، أو تعطيلها، أو تدمير البرامج، أو حذفها، أو إتلافها، أو تعديلها، يعاقب بالأشغال الشاقة المؤقتة وبغرامة مالية لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (7)

كل من التقط ما هو مرسل عن طريق الشبكة، أو إحدى وسائل تكنولوجيا المعلومات، أو سجله، أو اعترضه، أو تنصت عمداً دون وجه حق، يعاقب بالحبس، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (8)

1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية، أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس أو بالغرامة التي لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.
3. كل من ارتكب جريمة باستخدام أي من المذكور في الفقرة (2) من هذه المادة، يعاقب بالأشغال الشاقة المؤقتة وبالغرامة التي لا تقل عن ألفي دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9)

1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. إذا كان الانتفاع المحدد في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بالغرامة التي لا تقل عن ألف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

المادة (10)

كل من قام عمداً بإنشاء أو نشر شهادة غير صحيحة، أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة، أو إلغائها أو إيقافها، يعاقب بالحبس وبالغرامة التي لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (11)

1. كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة، أو الهيئات والمؤسسات العامة، معترفاً به قانوناً في نظام معلوماتي، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد عن عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
2. إذا وقع التزوير فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر يعاقب بالحبس أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
3. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأصول.
4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه، أو إتلافه، أو تعييبه، أو تعديله، أو تحويره، أو بأية طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته، أو معلوماته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبالغرامة التي لا تقل عن خمسة آلاف دينار أردني، ولا تزيد عن عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.
5. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
6. كل من أنشأ بيانا توقيع أو أداة نظام توقيع إلكتروني رسمي، أو للهيئات أو للمؤسسات العامة، لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (12)

1. كل من استخدم الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات في الوصول دون وجه حق إلى أرقام، أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من زور وسيلة تعامل إلكترونية بأية وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك، أو قبل وسيلة تعامل إلكترونية غير سارية، أو مزورة، أو مسروقة، أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
4. إذا قصد من ذلك استخدامها في الحصول على أموال أو بيانات غيره أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.
5. إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال غيره، يعاقب مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (13)
كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال، أو اختلاسها يعاقب بالأشغال الشاقة المؤقتة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كلتيهما.

مادة (14)
كل من توصل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات إلى الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني، أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (15)
1. كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف والاعتبار، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلهما بالعملة المتداولة قانوناً.

مادة (16)
1. كل من أنتج ما من شأنه المساس بالآداب العامة، أو أعده أو هيأه أو أرسله أو خزنه بقصد الاستغلال، أو التوزيع أو العرض على غيره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، أو الرسوم المتحركة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات؛ تدعو إلى تسهيل برامج وأفكار تروج لما من شأنه المساس بالآداب العامة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة مالية لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
3. إذا كان الفعل المحدد في الفقرتين (1،2) من هذه المادة موجهاً إلى طفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.
4. إذا كان محتوى الفعل الوارد في الفقرة (1) من هذه المادة طفل أو هيئة طفل أو صور محاكاة للطفل، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (17)
كل من أنشأ موقعاً أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاتجار في البشر والأعضاء البشرية أو تسهيل التعامل فيه، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (18)
دون الإخلال بالأحكام الواردة في قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب، كل من أنشأ موقعاً، أو تطبيقاً أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد ارتكاب جريمة غسل الأموال وتمويل الإرهاب،

يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (19)

كل من أنشأ موقعاً على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات والمؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو لبيعها، أو شرح، أو عرض طرق إنتاج المواد المخدرة، يعاقب بالحبس مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (20)

1. كل من أنشأ موقعا إلكترونياً، أو أداره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد نشر أخبار من شأنها تعريض سلامة الدولة، أو نظامها العام، أو أمنها الداخلي أو الخارجي للخطر، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من روّج بأية وسيلة تلك الأخبار بالقصد ذاته أو بثها أو نشرها، يعاقب بالحبس مدة لا تزيد على سنة، أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد عن ألف دينار أردني، أو بالعقوبتين كلتيهما.
3. إذا كان الفعل الوارد في الفقرتين (1،2) من هذه المادة في حالة الطوارئ تضاعف العقوبة المقررة له.

مادة (21)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الإساءة أو سب إحدى المقدسات أو الشعائر المقررة للأديان، أو أحد المعتقدات الدينية، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (22)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاعتداء على أي من المبادئ أو القيم الأسرية، من خلال نشر أخبار، أو صور، أو تسجيلات صوتية أو مرئية، سواء أكانت مباشرة أو مسجلة تتصل بحرمة الحياة الخاصة، أو العائلية للأفراد ولو كانت صحيحة، أو تعدى بالذم، أو القدح، أو التحقير أو التشهير بالآخرين وإلحاق الضرر بهم، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (23)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة، أو تسهيله، أو تشجيعه، أو الترويج له، أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (24)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد نشر وتوزيع معلومات تثير النعرات العنصرية، وتهدف إلى التمييز العنصري بحق فئة معينة، أو أقدم على تهديد شخص، أو تحقيره، أو التعدي عليه بسبب انتمائه العرقي أو المذهبي، أو اللون، أو الشكل، أو سبب الإعاقة، يعاقب بالأشغال الشاقة المؤقتة، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشر آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (25)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التبرير لأعمال إبادة جماعية، أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية، أو المساعدة قصداً، أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالأشغال الشاقة المؤبدة، أو الأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات.

مادة (26)

كل من حاز جهازاً بغرض الاستخدام، أو برنامجاً، أو أية بيانات إلكترونية معدة، أو كلمة سر، أو تراميز دخول، أو قدمها، أو أنتجها، أو وزعها، أو استوردها، أو صدرها، أو روّج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (27)

1. كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون مستغلاً صلاحياته وسلطته في أثناء تأدية عمله، أو بسببها أو سهل ذلك لغيره، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو بالعقوبتين كلتيهما.
2. كل من ارتكب من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون في أثناء تأدية عمله، أو بسببها، أو سهل ذلك لغيره، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن ثلاث سنوات، أو بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو بالعقوبتين كلتيهما.

مادة (28)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات؛ بقصد ارتكاب أية جريمة معاقب عليها بموجب أي تشريع نافذ، أو اشترك أو حرض على ارتكابها، يعاقب بضعف العقوبة المنصوص عليها في ذلك التشريع.

مادة (29)

1. كل من حرض، أو ساعد، أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون بأية وسيلة إلكترونية، ووقعت الجريمة بناءًعلى هذا التحريض أو المساعدة، أو الاتفاق، يعاقب بثلثي الحد الأقصى للعقوبة المقررة لفاعلها.
2. إذا كان المجني عليه طفلا في الفقرة (1) من هذه المادة، يعاقب المجرم بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، ولو لم تقع الجريمة فعلا.

مادة (30)

إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالغرامة التي لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات، أو أن تقضي بحله وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له.

مادة (31)

يعاقب بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني كل من قام باستخدام أنظمة أو موقع أو تطبيق إلكتروني؛ لتجاوز الحجب المفروض بموجب أحكام هذا القرار بقانون.

مادة (32)

يلتزم مزود الخدمة، وفقاً للإجراءات القانونية المقررة بالآتي:

1. تزويد الجهات المختصة بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية مع مراعاة الإجراءات الواردة في المادة (40) من هذا القرار بقانون.
3. الاحتفاظ بالمعلومات عن المشترك لمدة لا تقل عن ثلاث سنوات.
4. التعاون ومساعدة الجهات المختصة، وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ بها.

مادة (33)

1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
2. يجب أن يكون أمر التفتيش مسبباً ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.
3. إذا أسفر التفتيش المحدد في الفقرة (2) من هذه المادة عن ضبط أجهزة، أو أدوات، أو وسائل ذات صلة بالجريمة؛ يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها.
4. لوكيل النيابة العامة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أية وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.
5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

مادة (34)

1. للنيابة العامة الحصول على الأجهزة، أو الأدوات، أو الوسائل، أو البيانات، أو المعلومات الإلكترونية، أو بيانات المرور، أو البيانات المتعلقة بحركة الاتصالات، أو بمستعمليها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.
2. للنيابة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات، أو جزء منه، أو أية وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.
3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضرورياً، أو تعذر إجراؤه؛ تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.
4. إذا استحال إجراء الضبط والتحفظ عليه بصفة فعلية؛ وحفاظاً على أدلة الجريمة يتعين استعمال كافة الوسائل المناسبة؛ لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات.
5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه بما في ذلك الوسائل الفنية لحماية محتواها.
6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم، أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويُحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف، أو مغلف مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

مادة (35)

1. لقاضي الصلح أن يأذن للنيابة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديدة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى النيابة العامة.
2. للنيابة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركات الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.

مادة (36)

على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة، أو الأدوات، أو وسائل تكنولوجيا المعلومات، أو الأنظمة الإلكترونية، أو البيانات، أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها.

مادة (37)

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له ومدته.
2. تكون مدة الاعتراض المحدد في الفقرة (1) من هذه المادة ثلاثة شهور من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.
3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (38)

لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية، بسبب طبيعة ذلك الدليل.

مادة (39)

لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى لمجرد ذلك السبب، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي.

مادة (40)

1. لجهات التحري والضبط المختصة - إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو صور، أو أفلام، أو أية مواد دعائية، أو غيرها، من شانها تهديد الأمن القومي، أو السلم الأهلي، أو النظام العام، أو الآداب العامة - أن تعرض محضراً بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية، أو حجب بعض روابطها من العرض.
2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال 24 ساعة مشفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو بالرفض.

مادة (41)

فيما عدا الالتزامات المهنية المنصوص عليها في القانون لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها؛ للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقاً لأحكام القانون.

مادة (42)

تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.
2. الإسراع في إبلاغ الجهة المختصة عن أية جريمة منصوص عليها في هذا القرار بقانون فور اكتشافها أو اكتشاف أية محاولة للالتقاط، أو الاعتراض، أو التنصت بشكل غير مشروع وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة.

3. الاحتفاظ ببيانات تكنولوجيا المعلومات ومعلومات المشترك لمدة لا تقل عن 120 يوماً وتزويد الجهة المختصة بتلك البيانات.
4. التعاون مع الجهات المختصة لتنفيذ اختصاصاتها.

مادة (43)

1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال وتفادي ارتكابها والمساعدة على التحقيق فيها وتتبع مرتكبيها.
2. يتوقف التعاون المشار إليه بالفقرة (1) من هذه المادة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

مادة (44)

1. يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقاً للقواعد التي يقررها قانون الإجراءات الجزائية والاتفاقيات الثنائية، أو متعددة الأطراف التي تكون الدولة طرفاً فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر.
2. لا ينفذ طلب المساعدة القانونية، أو طلب تسليم المجرمين، استناداً إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها، أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرماً بمقتضى قوانين الدولة الطالبة.

مادة (45)

مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات النافذ، أو أي قانون آخر يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات المنصوص عليها فيه.

مادة (46)

كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها، أو تدخل، أو حرض على ارتكابها، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (47)

كل من أنشأ موقعاً على الشبكة الإلكترونية، يهدف إلى الترويج لارتكاب أية جريمة من الجرائم المنصوص عليها في قانون العقوبات، أو أي من القوانين الخاصة، يعاقب بالسجن المؤقت وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (48)

كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على ثلاثة آلاف دينار أردني أو بإحدى هاتين العقوبتين.

مادة (49)

كل من أقدم على العبث بأدلة قضائية معلوماتية، أو أقدم على إتلافها، أو إخفائها، أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (50)

كل من امتنع عن قصد في الإبلاغ، أو أبلغ عن قصد بشكل خاطئ عن جرائم معلوماتية، يعاقب بالحبس مدة لا تقل عن ستة شهور، وبغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني أو بإحدى هاتين العقوبتين.

مادة (51)

إذا وقعت أية جريمة من الجرائم المنصوص عليها في هذا القرار بقانون بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو تعريض حياة المواطنين للخطر، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القانون الأساسي أو القوانين أو اللوائح، أو بقصد الإضرار بالوحدة الوطنية، والسلام الاجتماعي، أو ازدراء الأديان أو الاعتداء على الحقوق والحريات التي يكفلها الدستور أو القانون الأساسي، تكون العقوبة الأشغال الشاقة المؤبدة أو المؤقتة.

مادة (52)

يعاقب من يشترك بطريق الاتفاق أو التحريض، أو المساعدة، أو التدخل في ارتكاب جناية، أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب عليها بنصف العقوبة المقررة لها.

مادة (53)

يعد مرتكبا لجريمة الشروع كل من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها، في هذا القرار بقانون ويعاقب بنصف العقوبة المقررة لها.

مادة (54)

1. دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حَسَن النية، تصدر المحكمة قراراً بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون، أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل.
2. تصدر المحكمة قراراً بمدة إغلاق المحل وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.

مادة (55)

تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أيا من الجرائم المنصوص عليها فيه سواء ارتكبت في فلسطين أم خارجها، وتعتبر الأحكام الأجنبية سابقة التكرار بحق الجاني.

مادة (56)

تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون في أي من الحالات الآتية:

1. إذا ارتكبها أو سهل ارتكابها موظف في مؤسسة خاصة، أو موظف عام مستغلا صلاحياته وسلطاته في ذلك، أو من في حكمه، كما يحكم على الموظف العام بالفصل من الوظيفة في حال الإدانة.
2. إذا وقعت الجريمة على موقع، أو نظام معلوماتي، أو بيانات، أو أرقام، أو حروف، أو شفرات، أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها بما في ذلك الهيئات المحلية.
3. أرتكاب الجاني الجريمة من خلال عصابة منظمة.
4. التغرير بالأحداث ومن في حكمهم واستغلالهم.
5. إذا وقعت الجريمة على نظام معلومات، أو موقع إلكتروني، أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع والتقاص، أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

مادة (57)

يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة وأدى إلى ضبط باقي الجناة.

مادة (58)

تتولى الوزارة وفقا لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون.

مادة (59)

يلغى كل ما يتعارض مع أحكام هذا القرار بقانون.

مادة (60)

يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره.

مادة (61)

على الجهات المختصة كافة، كل فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية.

صدر في مدينة رام الله بتاريخ: 24/06/2017 ميلادية
الموافق: 29/رمضان/2017 هجرية

محمود عباس
رئيس دولة فلسطين
رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

قوانين

قانون رقم 09 – 04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

إن رئيس الجمهورية،

– بناء على الدستور، لا سيما المواد 119 و120 و122 – 7 و126 منه،

– وبمقتضى الأمر رقم 66 – 155 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 66 – 156 المؤرّخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 75 – 58 المؤرّخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمتضمن القانون المدني، المعدّل والمتمّم،

– وبمقتضى القانون رقم 2000 – 03 المؤرّخ في 5 جمادى الأولى عام 1421 الموافق 5 غشت سنة 2000 الذي يحدّد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المعدّل والمتمّم،

– وبمقتضى الأمر رقم 03 – 05 المؤرّخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003 والمتعلق بحقوق المؤلف والحقوق المجاورة،

– وبمقتضى القانون رقم 08 – 09 المؤرّخ في 18 صفر عام 1429 الموافق 25 فبراير سنة 2008 والمتضمن قانون الإجراءات المدنية والإدارية،

– وبعد رأي مجلس الدولة،

– وبعد مصادقة البرلمان،

يصدر القانون الآتي نصه :

الفصل الأول
أحكام عامة

الهدف

المادّة الأولى : يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المصطلحات

المادّة 2 : يقصد في مفهوم هذا القانون بما يأتي :

أ – الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية،

ب – منظومة معلوماتية : أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين،

ج – معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها،

د – مقدمو الخدمات :

1 – أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،

2 – وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها،

هـ – المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة،

و – الاتصالات الإلكترونية : أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

مجال التطبيق

المادّة 3 : مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفصل الثاني
مراقبة الاتصالات الإلكترونية

الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية

المادّة 4 : يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات الآتية :

أ – للوقاية من الأفعال الموصوفة بجرائم الإرهاب أوالتخريب أوالجرائم الماسة بأمن الدولة،

ب – في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

ج – لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية،

د – في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة "أ " من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه، إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة "أ " من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

الفصل الثالث
القواعد الإجرائية

تفتيش المنظومات المعلوماتية

المادّة 5 : يجوز للسلطات القضائية المختصة وكذا ضبّاط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه، الدخول، بغرض التفتيش، ولو عن بعد، إلى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب – منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ " من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

حجز المعطيات المعلوماتية

المادّة 6 : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة

تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

الحجز عن طريق منع الوصول إلى المعطيات

المادّة 7 : إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

المعطيات المحجوزة ذات المحتوى المجرم

المادّة 8 : يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة ، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

حدود استعمال المعطيات المتحصل عليها

المادّة 9 : تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.

الفصل الرابع

التزامات مقدمي الخدمات

مساعدة السلطات

المادّة 10 : في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

حفظ المعطيات المتعلقة بحركة السير

المادّة 11 : مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج – الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د – المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

هـ – المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ " من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج.

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات.

تحدد كيفيات تطبيق الفقرات 1 و2 و3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

الالتزامات الخاصة بمقدمي خدمة "الإنترنت"

المادّة 12 : زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي خدمات "الإنترنت" ما يأتي :

أ – التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن،

ب – وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

الفصل الخامس

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته

إنشاء الهيئة

المادّة 13 : تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

مهام الهيئة

المادّة 14 : تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام الآتية :

أ – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

ب – مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،

ج – تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

الفصل السادس

التعاون والمساعدة القضائية الدولية

الاختصاص القضائي

المادّة 15 : زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني.

المساعدة القضائية الدولية المتبادلة

المادّة 16 : في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أوالبريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

تبادل المعلومات واتخاذ الإجراءات التحفظية

المادّة 17 : تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية ومبدأ المعاملة بالمثل.

القيود الواردة على طلبات المساعدة القضائية الدولية

المادّة 18 : يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب.

المادّة 19 : ينشر هذا القانون في الجريدة الرّسميّة للجمهوريّة الجزائريّة الدّيمقراطيّة الشّعبيّة.

حرّر بالجزائر في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009.

عبد العزيز بوتفليقة

قائمة المصادر و المراجع

قائمة المصادر و المراجع

أولاً القوانين.

1. دولة فلسطين، قانون حقوق الطبع البريطاني لسنة 1911 المطبق على فلسطين بموجب المرسوم الملكي المؤرخ في 1924/3/21 المسمى بقانون حقوق الطبع والتأليف.
2. دولة فلسطين، قانون العقوبات رقم 74 لسنة 1936 النافذ في المحافظات الجنوبية (قطاع غزة).
3. دولة فلسطين، قانون العقوبات رقم 16 لسنة 1960 الأردني المطبق في الضفة الغربية.
4. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-155 المؤرخ في 8 يوليو 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم، الجريدة الرسمية العدد 48، الجزائر، 1966.
5. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 66-156 المؤرخ في 8 يوليو 1966 المتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية العدد 48، الجزائر، 1966.
6. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني المعدّل والمتمم، الجزائر، 1975.
7. دولة فلسطين، قانون رقم(3) لسنة 1996 بشأن الاتصالات السلكية واللاسلكية، جريدة الوقائع الفلسطينية العدد12، فلسطين، 1996.
8. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 2000-03 المؤرخ في 5 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية العدد48، الجزائر، 2000.
9. دولة فلسطين، قانون الاجراءات الجزائية رقم 3 لسنة 2001.
10. الجمهورية الجزائرية الديمقراطية الشعبية، الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة له المؤرخ في 2003/7/19 المعدل والمتمم للأمر رقم 14/73، الجريدة الرسمية ، الجزائر، 2003.
11. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 05-01 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الطبعة الاولى، الديوان الوطني للأشغال التربوية، الجزائر،2005.

12. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 5 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد47، الجزائر، 2009.

13. دولة فلسطين، القانون المدني الفلسطيني رقم 4 لسنة 2012 المؤرخ في 2012/8/5، جريدة الوقائع الفلسطينية عدد ممتاز، فلسطين،2012.

14. الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 15-06 المؤرخ في 15 فبراير 2015 يعدل ويتمم القانون رقم 05-01 المتعلق بتبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية للجمهورية الجزائرية العدد 08، الجزائر، 2015.

15. دولة فلسطين، قرار بقانون رقم 20 لسنة 2015م بشأن مكافحة غسل الأموال وتمويل الإرهاب المؤرخ في 2015/12/30، جريدة الوقائع الفلسطينية عدد ممتاز10، فلسطين، 2015.

16. دولة فلسطين، القرار بقانون رقم 15 لسنة 2017 بشأن المعاملات الالكترونية المؤرخ في 2017/7/9، جريدة الوقائع الفلسطينية عدد ممتاز14، فلسطين، 2017.

17. دولة فلسطين، القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية المؤرخ في 2017/7/9، جريدة الوقائع الفلسطينية العدد ممتاز14، فلسطين، 2017.

18. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15-261 المؤرخ في 8 اكتوبر2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الجزائر، 2015.

ثانياً: الكتب.

1.أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، مصر، 2006،

2. آمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، بدون رقم طبعة، دار هومة، الجزائر،2006.

3. الإسكوا الأمم المتحدة اللجنة الاقتصادية والاجتماعية لغربي آسيا، نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا، منظمة الأمم المتحدة، أمريكا، 2007.

4. حجازي عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، بدون رقم طبعة، دار النهضة العربية، مصر، 2009.

5. خالد مصطفى فهمي، الحماية القانونية لبرامج الكمبيوتر، بدون رقم طبعة، دار الجامعة الجديدة للنشر، مصر، 2005.

6. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، طبعة 2010، دار الهدى، الجزائر، 2010.

7. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، بدون رقم طبعة، دار الهدى، الجزائر،2011.

8. عبد الرحمان خلفي، الاجراءات الجزائية في التشريع الجزائري والمقارن، الطبعة الثالثة، دار بلقيس، الجزائر، 2017.

9. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، الطبعة الأولى، بهجات للطباعة والتجليد، مصر، 2009.

10. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي للنشر، مصر،2006.

11. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالكمبيوتر وأبعادها الدولية، الطبعة الثانية، دار النهضة العربية، مصر،1995.

12. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، بدون رقم طبعة، منشورات الحلبي الحقوقية، لبنان، 2003.

13. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، بدون رقم طبعة، دار الجامعة الجديدة للنشر، مصر، 1997.

14. محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، الطبعة الثانية، دار الثقافة للنشر والتوزيع، الأردن 2010.

15. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، بدون رقم طبعة، دار الجامعة الجديدة للنشر، مصر،2001.

16. مصطفى محمد موسى، التحقيق في الجرائم الإلكترونية، بدون رقم طبعة، مطابع الشرطة للنشر، مصر، 2009.

17. نبيل صقر، الوسيط في شرح جرائم الأموال، بدون رقم طبعة، دار الهدى، الجزائر، 2012.

ثالثاً: الرسائل والمذكرات.

أ- الأطروحات

1. إحسان طبال، النظام القانوني للتحقيق الدولي في جرائم الكمبيوتر، أطروحة دكتوراه في الحقوق، جامعة الجزائر1، الجزائر، السنة الجامعية 2013-2014.

2. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت دراسة مقارنة، أطروحة قدمت استكمالاً لمتطلبات منح الدكتوراه فلسفة تخصص القانون الجنائي، جامعة عمان العربية، الأردن، 2003.

ب- الرسائل

1. آمال قارة، الجريمة المعلوماتية، رسالة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر1، الجزائر، السنة الجامعية 2001-2002.

2. حقاص صونية، حماية الملكية الفكرية الأدبية والفنية في البيئة الرقمية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماجستير تخصص المعلومات الالكترونية الافتراضية واستراتيجية البحث عن المعلومات، جامعة منتوري قسنطينة، الجزائر، 2012.

3. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون الجنائي، جامعة الجزائر1، الجزائر، السنة الجامعية 2011-2012.

4. نبيل محمود فريد أبو الرب، مفهوم الجرائم الإلكترونية وتحدياتها التشريعية في فلسطين، أطروحة مقدمة استكمالاً للحصول على شهادة الماجستير في القانون العام، جامعة النجاح الوطنية، فلسطين، 2018.

ج- المذكرات

1. بوعوينة أمين شعيب، مهلب حمزة، اختصاصات لضبطية القضائية في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق شعبة القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة بجاية، السنة الجامعية 2012-2013.

2. صديق حياة، خصوصية الجريمة المعلوماتية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2008.

3. عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2013-2014.

4. قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة مكملة لمتطلبات شهادة الماستر أكاديمي تخصص قانون عام للأعمال، جامعة قاصدي مرباح ورقلة، السنة الدراسية 2013-2014.

5. قريم سكورة، المواجهة الإجرائية للجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في القانون تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند اولحاج البويرة، 2015.

6. كوداد عبد الرحمن، عملية التسرب على ضوء التشريع الجزائري، مذكرة نيل شهادة الماستر في الحقوق تخصص علم الإجرام، جامعة الطاهر مولاي سعيدة، الجزائر، السنة الجامعية 2016-2017.

7. لعاقل فريال، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون العام تخصص القانون الجنائي والعلوم الجنائية، جامعة أكلي محند اولحاج-البويرة، الجزائر، 2014-2015.

8. مخلوف عكاشة، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور مولاي الطاهر سعيدة، الجزائر، السنة الجامعية 2016-2017.

9. مهدي شمس الدين، النظام القانوني للتسرب في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، جامعة محمد خيضر بسكرة، الجزائر، السنة الجامعية 2013-2014.

رابعاً: المؤتمرات.

1. آمال بن صويلح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة في الملتقى الوطني الدولي حول" الإجرام السيبراني المفاهيم والتحديات"، جامعة 8 ماي 1945 قالمة، المنعقد يومي 11-12 افريل 2017، الجزائر، 2017.

2. عاقلي فضيلة، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مداخلة في المؤتمر الدولي الرابع عشر: طرابلس 24-25 مارس 2017، لبنان، 2017.

خامساً: المحاضرات.

1. إحسان طبال، محاضرات ملقاة على طلبة السنة ثانية ماستر ، قانون جنائي وعلوم جنائية، جامعة يحي فارس بالمدية، 2018/2017.

2. بن دعاس فيصل، إشكالات الجريمة المعلوماتية في التشريع الجزائري، محاضرة في إطار التكوين المحلي المستمر للقضاة، الجزائر، السنة القضائية 2010-2011.

سادساً: المجلات.

1. بوعناد فاطمة زهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، الجزائر، 2013.
2. زوزو هدى، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، العدد الحادي عشر، 2014.
3. محمد موسى خلف، حماية برامج الحاسب الآلي بين براءة الاختراع وحق المؤلف، مجلة الفكر، العدد الثالث عشر، جامعة محمد خيضر بسكرة، بدون سنة نشر.

سابعاً: المواقع الإلكترونية.

1. http://www.palpolice.ps/ar ، تاريخ الاطلاع 2018/3/17.
2. http://www.startimes.com/?t=14565170 ، تاريخ الاطلاع 2018/3/6.

الفهرس

الفهرس

العنوان	الصفحة
مقدمة	02
الفصل الأول: الإطار الموضوع للجريمة المعلوماتية.	**06**
المبحث الأول: المكافحة الموضوعية للجريمة المعلوماتية في قانون العقوبات.	07
المطلب الأول: تطويع النصوص الجنائية التقليدية.	07
الفرع الأول: مدى انطباق وصف المال على المعلوماتية.	07
الفرع الثاني : مدى اعتبار البرامج مالاً بصدد جرائم الأموال	12
الفرع الثالث: النشاط الاجرامي لجرائم الاموال والمعلوماتية.	15
المطلب الثاني: ضرورة استحداث نصوص جنائية خاصة تعنى بالجريمة المعلوماتية.	23
الفرع الأول: استحداث نصوص جنائية خاصة في قانون العقوبات الجزائري.	23
الفرع الثاني: انعدام النصوص الجنائية في قانون العقوبات الفلسطيني.	30
المبحث الثاني: المكافحة الموضوعية للجريمة المعلوماتية في ظل القوانين الخاصة.	33
المطلب الأول: الحماية الجنائية في القوانين المكملة لقانون العقوبات.	33
الفرع الأول: الحماية الجنائية في القوانين المكملة لقانون العقوبات الجزائري.	34
الفرع الثاني: الحماية الجنائية في القوانين المكملة لقانون العقوبات الفلسطيني.	37
المطلب الثاني: الحماية الجنائية في النصوص المتعلقة بالملكية الفكرية.	46
الفرع الأول: الحماية من خلال نصوص الملكية الفكرية في التشريع الجزائري	46
الفرع الثاني: الحماية الجنائية من خلال نصوص الملكية الفكرية في التشريع الفلسطيني.	50
خلاصة الفصل.	56
الفصل الثاني: الإطار الإجرائي للجريمة المعلوماتية	**58**
المبحث الأول: المكافحة الإجرائية للجريمة المعلوماتية في ظل قانون الاجراءات الجزائية.	59
المطلب الأول: قواعد الاختصاص القضائي.	59
الفرع الأول: اختصاص المحاكم.	59
الفرع الثاني: اختصاص الضبطية القضائية.	60
الفرع الثالث: اختصاص النيابة العامة.	62

الفرع الرابع: اختصاص قاضي التحقيق.	63
الفرع الخامس: القانون واجب التطبيق.	65
المطلب الثاني: أعمال التحقيق.	69
الفرع الأول: التسرب.	69
الفرع الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.	71
المبحث الثاني: المكافحة الإجرائية للجريمة المعلوماتية في ظل القوانين الخاصة.	77
المطلب الأول: أعمال التحقيق الخاصة.	77
الفرع الأول: أعمال التحقيق المشتركة بين القانون الجزائري رقم 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الإعلام والاتصال والقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية.	77
الفرع الثاني: مراقبة الاتصالات الإلكترونية.	83
الفرع الثالث: الضبط المعلوماتي.	85
الفرع الثاني: أعمال التحقيق الخاصة بالقرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الإلكترونية الفلسطيني.	87
المطلب الثاني: إنشاء هيئات متخصصة والتعاون الدولي.	89
الفرع الأول: الهيئات المتخصصة في التشريع الجزائري.	90
الفرع الثاني: الهيئات المتخصصة في التشريع الفلسطيني.	93
الفرع الثالث: التعاون الدولي.	95
خلاصة الفصل :	100
خاتمة	102
الملاحق	-
قائمة المراجع	107
الفهرس	112